2011-12

Intelligence-led risk management for homeland security: a collaborative approach for a common goal

Jackson, David P.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTELLIGENCE-LED RISK MANAGEMENT FOR HOMELAND SECURITY: A COLLABORATIVE APPROACH FOR A COMMON GOAL

by

David P. Jackson

December 2011

Thesis Co-Advisors: Erik Dahl
Glen Woodbury

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Intelligence-Led Risk Management for Homeland Security: A Collaborative Approach for a Common Goal		**5. FUNDING NUMBERS**	
6. AUTHOR(S) David P. Jackson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The concept of risk management provides the foundation of the homeland security enterprise. The United States of America faces numerous complex risks ranging from a series of natural hazards, pandemic disease, technological hazards, transnational criminal enterprises and acts of terrorism perpetrated by intelligent adversaries. The management of these risks requires a strategic collaborative effort from the intelligence and risk analysis communities and many stakeholders at all levels of government, including the private sector. Paradoxically, a decentralized collaborative approach to homeland security risk management may produce better results than a hierarchical central approach driven by the U.S. Department of Security, as this thesis suggests. Intelligence-Led Risk Management represents the fusion of intelligence with risk management in a collaborative framework to promote effective risk management throughout the homeland security enterprise. Concepts from strategic thought and planning, such as the Cynefin Framework, Appreciative Inquiry, and Quantum Planning provide vehicles to promote collaboration and thoroughly explore the spectrum of risk management options available to the homeland security enterprise. Decentralization of homeland security risk management to states with the application of Intelligence-Led Risk Management through the network of fusion centers will promote collaboration and yield a stronger risk management culture within the homeland security enterprise.

14. SUBJECT TERMS Risk; Risk Management; Risk Analysis; Intelligence; Risk Ranking; Mitigation; Fusion Centers; Collaboration; Complexity; Terrorism; Natural Hazards; Intelligence-Led Risk Management; Strategy			**15. NUMBER OF PAGES** 145
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INTELLIGENCE-LED RISK MANAGEMENT FOR HOMELAND SECURITY: A COLLABORATIVE APPROACH FOR A COMMON GOAL

David P. Jackson
Critical Infrastructure Protection Program Manager / Fusion Center Liaison Officer
State of Idaho Bureau of Homeland Security
B.S., University of North Texas, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: David P. Jackson

Approved by: Erik Dahl, PhD
Thesis Co-Advisor

Glen Woodbury
Thesis Co-Advisor

Daniel Moran, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The concept of risk management provides the foundation of the homeland security enterprise. The United States of America faces numerous complex risks ranging from a series of natural hazards, pandemic disease, technological hazards, transnational criminal enterprises and acts of terrorism perpetrated by intelligent adversaries. The management of these risks requires a strategic collaborative effort from the intelligence and risk analysis communities and many stakeholders at all levels of government, including the private sector. Paradoxically, a decentralized collaborative approach to homeland security risk management may produce better results than a hierarchical central approach driven by the U.S. Department of Security, as this thesis suggests. Intelligence-Led Risk Management represents the fusion of intelligence with risk management in a collaborative framework to promote effective risk management throughout the homeland security enterprise. Concepts from strategic thought and planning, such as the Cynefin Framework, Appreciative Inquiry, and Quantum Planning provide vehicles to promote collaboration and thoroughly explore the spectrum of risk management options available to the homeland security enterprise. Decentralization of homeland security risk management to states with the application of Intelligence-Led Risk Management through the network of fusion centers will promote collaboration and yield a stronger risk management culture within the homeland security enterprise.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CRO	Chief Risk Officer
DHS	U.S. Department of Homeland Security
DMA	Disaster Mitigation Act of 2000
FEMA	Federal Emergency Management Agency
EMAP	Emergency Management Accreditation Program
EPA	Environmental Protection Agency
GAO	Government Accountability Office
ISO	International Organization for Standardization
NEMA	National Emergency Management Association
NIPP	National Infrastructure Protection Plan
NRC	Nuclear Regulatory Commission
NWS	National Weather Service
OMB	Office of Management and Budget
QHSR	Quadrennial Homeland Security Review Report
SLFCs	State and Local Fusion Centers
TCL	Target Capabilities List
USACE	U.S. Army Corps of Engineers
USGS	U.S. Geological Survey

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This work is dedicated to my many friends and colleagues within the homeland security and emergency management community. Their continued commitment to protect the citizens they serve amidst many significant challenges continues to inspire me.

First of all, I would like to thank my wife, Cathy. She has been my greatest champion supporting me every step of the way throughout this entire master's program. I would also like to thank my advisor, Erik Dahl, and second reader Glen Woodbury. Their patience and sage guidance throughout this process saw me through to the end. Additionally, my heartfelt thanks go to my family, friends, classmates, and colleagues at the Idaho Bureau of Homeland Security for their continued support throughout this educational odyssey. Finally, I extend my sincere appreciation to the Director of the Idaho Bureau of Homeland Security, Brigadier General Bill Shawver, who afforded me the opportunity to complete the program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT – BACKGROUND

Risk management is an essential component of the homeland security enterprise, but it is significantly fragmented and poorly coordinated among the numerous federal, state, local agencies, technical experts and private sector partners involved. This fragmentation and lack of coordination significantly detracts from a strategic approach for managing the wide range of risk within the homeland security enterprise.

The Department of Homeland Security's *DHS Risk Lexicon* defines risk management as, "the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost." (United States. Department of Homeland Security (DHS), 2010). Several recent publications offer support for the need to identify ways of improving the risk analysis and risk management process within the homeland security enterprise. The National Emergency Management Association (NEMA) outlines a strategic view to enhance risk management through broadening collaborative partnerships, increasing the level of total hazard awareness, and emphasizing a full spectrum community to federal approach to risk management (National Emergency Management Association, 2009).

Further justification for research in this area can be found in the DHS *Nationwide Plan Review,* which calls for the development of a comprehensive risk management process that is usable by all levels of government (Federal Emergency Management Agency (FEMA), 2010). The *Quadrennial Homeland Security Review Report* (QHSR) published in 2010 also identifies strategic goals and objectives to enhance the assessment and understanding of risk within the homeland security context. The problem of developing a standard approach to facilitate risk management across the homeland security enterprise that presents utility at each level of government and with private sector partners remains exceptionally complex. The complexity of this problem is the product of the many different threats, hazards, vulnerability characteristics, and unique specialized assessment tools.

The existing approach to risk assessment and management is too hierarchical and centralized at the federal level of government. The current homeland security risk assessment and management process, as it applies to state and local governments, is focused on supporting federal decisions related to the distribution of grant funds, which provide the primary means for the federal government to influence homeland security priorities within state and local government (Masse, T, Rollins, J, & O'Neil, S, 2007). This limited top-down perspective of risk management does not facilitate collaborative approach to assess and manage homeland security risks with state, local, and private sector partners. The Department of Homeland Security recognizes the need to include more state and local input into the risk assessment and management process, but it does not appear to have a clearly defined plan of how to accomplish this (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). This suggests that a decentralized approach to risk assessment and management focused within the construct of state and local government will improve national homeland security risk management. A compendium of risk assessment and management guidance, a suite of risk specific assessment tools, and access to technical experts to support state and local driven risk assessment and management strategies are needed to achieve a whole-of-nation approach to homeland security risk management.

Intelligence remains an important aspect of homeland security risk assessment and management. Improved collaboration between homeland security risk analysts and the intelligence community is critical for producing effective threat assessments that provide utility in assessing and managing homeland security risk. The need to improve cross discipline collaboration between the intelligence community and risk assessment / management community exists, and greater collaboration between the two disciplines will advance the quality of threat assessments and thus risk management within the homeland security enterprise (Baker et al., 2009). Greater collaboration between risk analysts and the intelligence community will also provide the opportunity to improve intelligence analysis (Willis, 2007). State and major urban area fusion centers provide a framework to facilitate collaboration between the intelligence community and risk analysts to support a decentralized approach to risk management driven by state and local

priorities. The prescribed capabilities for state and major urban area fusion centers suggest that the fusion centers can provide a structure to support this idea (United States. Department of Homeland Security, 2008).

A multi-disciplinary coalition or alliance at each tier of government could provide a mechanism to coordinate risk management among different disciplines and agencies into a common voice instead of the current fragmented structure of competing autonomous entities that address certain aspects of homeland security risk. While the entirety of risk management is too diverse and complex to be wholly managed by any one organization, a collaborative alliance can provide a governance structure to support the efforts of the fifty states and U.S. Territories and the U.S. Department of Homeland Security to manage homeland security risk.

B. RESEARCH QUESTIONS

The primary question this thesis will examine is: How can the existing Homeland Security risk management framework be improved to better support decision making and allocation of resources within state and local governments?

More specifically, this thesis will consider the following questions: How could we achieve a higher degree of collaboration between the intelligence community and risk analysts to support risk management within state and local governments? What factors influence successful collaboration, and how do they fit within a strategic planning framework?

This thesis will attempt to support the following assertions:

- A decentralized approach to risk assessment and management that is focused within the construct of state and local government will improve national homeland security risk management.
- Improved collaboration between the intelligence community and the risk management community will improve the processes and products of both risk assessment and intelligence.
- The capacity for collaboration exists within many agencies, but this fact must be recognized and joined with principles of strategic planning to improve risk management within the homeland security enterprise.

C. SIGNIFICANCE OF RESEARCH

Exploring the issues associated with improving risk-based decision making is more important than ever. According to comments from the Comptroller General and Secretary of Homeland Security, the United States cannot afford to protect all things from all threats and hazards, therefore, critical decisions must be made about how to invest limited resources to achieve the greatest results (Jenkins, 2007 pp 1–2). The Comptroller General goes on to assert that the current fiscal policy of the United States is on an unstable course, and that course needs to be altered to avoid damage to the national economy, reduction in our standard of living, and damage to our national security (Jenkins, 2007 p. 12). Existing economic challenges at all levels of government present even more challenging resource allocation and prioritization decisions that continue to emphasize the importance of risk management in the decision-making process.

The concept of risk management emphasizes strategic decision making with a tendency to focus on proactive strategies that relate to prevention, protection and hazard mitigation activities within the homeland security context. FEMA defines hazard mitigation as "any sustained action taken to reduce or eliminate the long-term risk to human life and property from hazards." (Federal Emergency Management Agency (FEMA), 2007 p. 3). This definition is similar to the definition of risk management. Risk analysis and mitigation/prevention activities within the context of emergency management and homeland security programs are not afforded the same consideration for resources and improvement as preparedness, response, and recovery activities. Although this inequity of attention and resources is not new, the importance of evaluating this issue increases with our investment of treasure in homeland security programs. A simple review of the Target Capabilities List (TCL) shows the disparity between the level of attention placed on risk management and protection activities and those of preparedness and response activities (United States. Department of Homeland Security, 2007). This difference is noteworthy, since state and local government focus their homeland security investments towards improving their capability in accordance with the TCL. The 2010 QHSR also concludes that a shift of program emphasis from response and recovery to one of risk management and preparedness is needed in order to achieve the level of

resilience sought by the homeland security community (United States. Department of Homeland Security, 2010). The benefits of hazard mitigation are most effective when they are based on a long-term strategic plan developed through an inclusive process before a disaster occurs (Federal Emergency Management Agency (FEMA), 2007 p. 3).

The research in this thesis will address an identified gap in coordinating the risk management function throughout the homeland security enterprise. The analysis will identify strengths and weaknesses in implementing a coordinated and comprehensive approach to integrated risk management. The ultimate goal of this research is to provide a collaborative framework that will provide the necessary support to state and local governments in risk management. An improved framework will provide state and local government with technical assistance and guidance for risk assessment and management, which in turn will support resource allocation for strategic risk management.

D. RESEARCH METHODOLOGY

The overarching goal of this thesis research is to identify shortfalls within the existing approach to all-hazard risk management within the homeland security enterprise, and to identify how additional collaborative efforts can improve the risk management. It includes special focus on two sub-issues. The first being how to improve collaboration between the intelligence community and risk analysts, and the second being the impact of a decentralized strategic approach to risk management on strategic decision making within state and local government.

The research for this thesis includes aspects of both policy analysis and program evaluation. This approach fuses a formative program analysis with a multi-goal policy analysis to establish the frame for the thesis. These approaches are combined to analyze both strengths and shortfalls within three areas germane to the area of research. These areas include the existing frameworks for homeland security risk management, intelligence analysis done in support of risk assessment, and collaboration and strategic planning processes with application to the homeland security enterprise.

The first phase of research involves a qualitative/formative program analysis of the existing risk management framework used in the homeland security enterprise in the

United States. This identifies both strengths and weaknesses inherent to the homeland security risk management framework. The key attributes of several standards and guidance documents relevant to the homeland security risk management are compared in this analysis. This comparison includes: the Target Capabilities List published by the U.S. Department of Homeland Security in 2007, the Emergency Management Accreditation Program (EMAP) developed by the National Emergency Management Association (NEMA), the *Baseline Capabilities for State and Major Urban Area Fusion Centers, Critical Infrastructure and Key Resources Protection Capabilities for Fusion Centers* both published by the U.S. Department of Homeland Security in 2008, and FEMA's state and local hazard mitigation planning guidance. This phase includes identification of common themes and recommendations in recent reports and studies related to the risk management function within the homeland security discipline. It also examines the risk management components of the existing the DHS Risk Management Doctrine critical infrastructure protection program and the manner in which they are being implemented under the National Infrastructure Protection Plan. This examination includes the organization and role of state fusion centers with respect to risk management functions for both infrastructure protection and terrorism threats.

The second phase of research involves a qualitative/comparative program analysis of the intelligence cycle and risk management cycle. This analysis explores existing processes for collaboration between the intelligence community and risk analysts and seeks to identify the benefits and challenges inherent to this collaboration. The focus on state and local fusion centers (SLFCs) for this phase of research is important for two reasons. The first is based on SLFCs collaborative nature for gathering risk information, assessing threats, and communicating risk. The second reason is that SLFCs provide direct intelligence and analysis support to agencies with a homeland security mission within state and local government. The research conducted for this thesis and discussions

with colleagues in both the critical infrastructure program and hazard mitigation programs indicate that fusion centers remain focused on terrorism and criminal threats related to infrastructure protection.

The third phase of research entails exploration of the enabling and barrier factors to interagency collaboration within the homeland security community. It also identifies principles of strategic thought and planning and provides a comparison with those factors that enable collaboration. The research in this section focuses on the common traits associated with collaborative efforts and effective strategic planning within the homeland security enterprise. The analysis seeks to determine how positive traits and strategic planning principles can be applied to a new collaborative model for all hazard risk management within the homeland security enterprise. The analysis also seeks to understand negative aspects of collaboration and apply management and organizational theory to overcome identified barriers for collaboration.

The final aspect of the proposed methodology includes a multi-goal policy analysis to compile the information from the first three phases of research into a summary analysis of the risk management policy within the homeland security enterprise. The result of the multi-goal policy analysis includes recommendations for improvement and the identification of areas for additional research and study.

E. OVERVIEW OF CHAPTERS

As outlined in Chapter I, the introductory chapter, the focus of this thesis involves exploring ways to improve the risk management within homeland security through collaboration and decentralization of the risk management process. It employs a comparative program analysis to evaluate the existing risk management framework and collaboration between the intelligence and risk management communities.

Chapter II provides an overview of the homeland security risk management framework as it currently exists. The foundation provided in this chapter provides the basis for understanding the issues within the existing framework and for comparison for the remainder of the thesis. The challenges identified in this chapter provide an opportunity to improve the homeland security risk management framework. This second

chapter goes on to present a comparison of multiple risk management standards and models applicable to the homeland security enterprise. This comparison identifies the common themes and differences that exist within the various approaches to risk management employed throughout the homeland security enterprise. It also examines the concept of comparative risk assessment and its potential application to strategic risk management within homeland security.

Chapter III introduces the topic of intelligence as it relates to the homeland security enterprise and establishes the relationship between intelligence and risk assessment and management. This chapter provides a comparison of the intelligence cycle to the risk management cycle from the recently published *DHS Risk Management Doctrine* and the Carnegie Mellon Risk Ranking Model. The chapter provides a discussion on existing collaborative efforts between the intelligence community and risk analysis community. It goes on to examine potential mutual benefits of enhanced collaboration between intelligence and risk analysts. State and local fusion centers are also introduced to the discussion in this chapter. The fusion center discussion goes on to suggest that fusion centers can provide a vehicle to improve collaboration between intelligence and risk analysts in support of a decentralized strategic risk management model driven by state and local governments. In this context, the idea of Intelligence-Led Risk Management is introduced as a means to improve collaboration between intelligence and risk analysts to improve state and local decision making and strategic risk management.

The focus of Chapter IV involves a discussion on collaboration and strategic thought and planning. It begins by establishing that collaboration plays an essential role within the homeland security enterprise and more specifically an important role within the homeland security risk management process. The discussion progresses to include an analysis of factors that enable or stifle interagency collaboration. This discussion is based largely on the Inter-Organizational Collaborative Capacity Model developed by Hocevar, Jansen and Thomas. The concept of federalism is introduced to the conversation as a collaborative structure for government. The discussion on federalism draws comparisons with the enabling and barrier factors discussed earlier in the chapter. It goes on to explain

how friction between states and the federal government creates barriers to collaboration and the underlying reasons discouraging a decentralized approach for strategic risk management. The last portion of Chapter IV introduces strategic thought and planning concepts to the conversation. These concepts include Appreciative Inquiry, the Cynefin Framework, and other principles of strategic planning. These concepts are compared with the success and barrier factors from the Inter-Organizational Collaborative Capacity Model to identify strategies to enable collaboration and manage the obstacles to further strategic risk management.

F. LITERATURE REVIEW

1. Risk Management Literature

A significant volume of literature relating to risk management within the emergency management and homeland security fields has been published. This includes several general guidance documents published by FEMA on hazard mitigation planning and risk analysis, including the *DHS Risk Lexicon* first published in 2008 and updated in 2010, and the *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* published in 2011. The common elements of these documents involve hazard or threat identification and risk analysis as the fundamental elements of a strategic approach to risk management. These various documents also communicate the importance and value of considering all hazards and all threats, but they fail to provide details on how to assess the wide range of threats, hazards and facilities, and they do not provide direction for additional information. The language and terminology among these documents varies significantly underlining the lack of coordination among the different organizations involved in risk assessment.

There is a significant amount of academic, government, and trade literature related to risk management that spans multiple decades. The literature considered was narrowed to focus on risk management related to the evolution of the emergency management and homeland security discipline. This range of literary sources relating to risk assessment includes the following subgroups: natural hazards, terrorism, biological threats or vectors, and technological hazards, which include infrastructure failures. A

good number of significant contributions that directly pertain to the primary research question were published within the last five years, suggesting this remains an area of academic and government interest.

Several reports published over the last five years provided a foundation for exploring the research area summarized in this thesis. These include *Review of the Department of Homeland Security's Approach to Risk Analysis* published by the National Academies in 2010, and two volumes published in 2006: *Homeland Security Risk Assessment, Volume I: Setting,* and *Homeland Security Risk Assessment Volume II: Methods, Techniques and Tools*. These sources were selected because of their relatively recent publication dates, and their focus on the issue of risk assessment, which is central to the research question.

A cursory review of these sources supports the general conclusion that the assessment of risk from natural hazards is the most evolved due to the foundation of high-quality data sets and refined models. A key area for improvement related to this aspect of risk assessment within the homeland security enterprise includes support of long-term risk management and policy decisions with emphasis on social aspects and efforts to support local and regional decision making, and to avoid cascading failures of critical infrastructure (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

The consensus among all of the sources reviewed to date is that the assessment of the risk associated with terrorism is hard to model because of the large variance among independent variables. The second order social and economic effects of terrorism have been largely overlooked so far in accounting for the risk from terrorism (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 5). All sources also agree with the notion that risk assessment is a complex process that requires multiple types of expertise to be effective, and that noncollaborative approaches to risk management often leave unacceptable residual risk and do not achieve the desired results.

The current approach for risk management within the homeland security enterprise appears to be driven from the federal level with a primary purpose of allocating homeland security funding. The QHSR calls for a national-level homeland security risk assessment (United States. Department of Homeland Security, 2010 p. 66). The assessment of risk from state and local government—where the majority of exposure lies—does not figure significantly into this process. DHS acknowledges this fact and the need to include more state and local threat and hazard information in their assessments (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 59). A report from the Government Accountability Office (GAO) stipulates that the risk analysis model used by DHS includes both empirical risk measures and policy judgments in assigning risk values for the allocation of resources, and that the limitations of the vulnerability model used in the risk assessment significantly reduce its utility (GAO, 2008). The focus on assessing risk associated with terrorist attacks is clear throughout the GAO report, but the report also alludes to the fact that other risks should be taken into account in analyzing vulnerabilities. A recent white paper published by the National Emergency Management Association (NEMA) identifies the three strategic themes that include broader collaborative partnerships, total hazard awareness, and full spectrum community-to-federal emphasis. These themes present a framework for a reexamination of the way in which we assess and analyze risk, and the manner in which we prioritize the functions of risk analysis, mitigation/prevention, and preparedness (NEMA 2009 p. 2–3).

One finding in the recently published National Plan Review calls for the Department of Homeland Security to develop a risk assessment and management process that has utility to all levels of government (DHS FEMA National Plan Review 2010 p. 43). The need for an enterprise-wide national level risk assessment in order to enable risk-informed decision making is further articulated in the Quadrennial Homeland Security Review Report (HDS QHSR 2010 p. 66). These findings comport with the recommendations in the NEMA white paper and appear to be applicable to all levels of government in support of their homeland security roles.

Even though there are notable differences between risk management processes associated with the wide range of threats and hazards within homeland security, exploration of how to incorporate these assessments into a useful tool for decision makers at all levels of government is warranted. The application of leading-edge science and technology is a major factor that influences the analysis of natural and technological hazards, as well as the threat of terrorism throughout homeland security (Government Accountability Office (GAO), 2008). This need is described within the Quadrennial Homeland Security Review Report, and it could support a nationwide comprehensive all-hazard intelligence model to drive risk-based decision making at all levels of government for all hazards and threats.

The consensus of literature reviewed on the topic suggests the challenge of developing a universal approach to risk management in the homeland security enterprise is formidable. One perspective suggests that DHS should establish a Chief Risk Officer (CRO) to manage all homeland security risks (U.S. Government Accountability Office, 2008, p. 7). This approach is similar to the model used by large corporations and insurance companies. The other predominant point of view suggests that the complexity of homeland security risk management is too great for any one individual or office to effectively manage (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010. p. 8–14). The competing perspectives suggest the most effective approach may lie somewhere in the middle. All of the literature agrees that effective risk management requires greater coordination and collaboration.

2. Intelligence and Fusion Center Literature

Much has been written about fusion centers and the intelligence analysis function within the homeland security environment. The majority of this literature has been published since 2004 and does not have the maturity and breadth of other literature categories. The importance of the intelligence community and their analysis is an important factor in understanding the risk associated with terrorism and to develop an effective risk management framework. In the National Intelligence Strategy, the former Director of National Intelligence, Dennis Blair, asserted that the United States faces a

complex and rapidly shifting security landscape, and that persistence and agile adaptation are required to meet these challenges. The goals outlined in the National Intelligence Strategy that directly apply to analyzing the risk from terrorism could easily apply to risk analysis related to natural and technological hazards (ODNI 2009 pp. 1–5).

The secretive nature of law enforcement and the intelligence community appear to contribute to the challenge of assessing the terrorism threat effectively as part of a collaborative all-hazard system for risk assessment and management. This point comes through in the discussion on risk assessment capabilities in the *Baseline Capabilities for State and Major Urban Area Fusion Centers* published in 2008 (United States. Department of Homeland Security, 2008 p. 7). The human behavior variable and emotional social aspect of terrorism also contribute to the challenge of assessing risk, and subsequently providing an analytical product to assist policy makers in making critical decisions.

Academic and practical discussions over fusion centers provide more questions than answers. Even though the U.S. Department of Homeland Security has published guidelines for state fusion centers that provide a description of common capabilities, however, in a practical sense the capabilities, structure, function and roles of fusion centers differ significantly. Even the primary audience for fusion center products is a question for debate. When considering the mainstream view that local law enforcement should be intelligence collectors and analysts, and that tactical level intelligence is the primary role of fusion centers dissenting opinions are readily available. One such example would argue that local law enforcement does not have capacity to gather intelligence and analyze the information, but instead state fusion centers should focus on taking national intelligence products and brief state and local executives on how they apply for the pertinent jurisdiction (Steiner 2009).

The intelligence analysis process may provide some interesting concepts that could apply to a comprehensive all-hazard all-risk management framework. This notion is supported with several recent publications. A recent publication by the Homeland Security Institute provides several findings and recommendations related to collaboration between the intelligence community and the risk analysis community. This report

provides a good foundation from which to understand the challenges and opportunities for collaboration between risk analysts and the intelligence community. Additionally, Henry Willis suggests that the risk analysis community can help improve the intelligence process (Willis, 2007). The fusion center process provided in the DHS guidelines provides an example that could provide a foundation for a framework to consider (United States. Department of Homeland Security, 2008). The importance of human intelligence and behavior could offer insights on ways to improve the social aspect of risk assessment and management. Even information sharing strategy for the U.S. Intelligence community calls for a collaborative transformation that promotes a cultural change from "need to know" to one that embraces a mindset of "responsibility to share" (United States Office of the Director of National Intelligence, 2008).

3. Collaboration and Strategic Planning Literature

A large volume of literature exists on the topic of collaboration and strategic planning. To manage the scope of this research project, the literature considered will relate to collaboration in government, public and private sector partnerships, and strategic planning. Significant research on collaboration in government and with public private sector partnerships exists largely due to public demand for more efficient government and the evolution of the homeland security enterprise.

A 2006 publication, "*Building Collaborative Capacity: An Innovative Strategy for Homeland Security Preparedness*" by Susan Page Hocevar and Gail Fann Thomas provides a strong and relevant starting position to examine how interagency collaboration can improve the risk management framework. Their work examines factors within homeland security organizations that both foster and deter effective inter-organizational collaboration. This work provides a suitable frame for identifying critical factors and obstacles for collaboration from which to conduct additional research on how to apply the positive factors into an organizational framework and to develop strategies to overcome the barriers.

Intergovernmental collaboration in the homeland security context takes place within the confines of the American system of federalism, which serves as the basis for our government. The literature suggests that federalism both enables and inhibits collaboration between tiers of government for homeland security. A review of the strategies and reports related to risk management and intelligence conveys a theme of the need for greater state and local input into the enterprise; however, collaboration remains difficult within the federalism context. This is largely due to the on-going struggle for power between the states and federal government. The problems of homeland security tend to exacerbate this friction as the times of crisis such as the Civil War, the Great Depression, and the Terrorist Attacks of 9/11 are shown to centralize more power in the federal government (Clovis, 2006).

The body of literature relating to strategic management fits nicely with the literature on collaboration for the purpose of examining ways to improve collaboration for strategic risk management within the homeland security community. The literature on the Cynefin Framework provides a useful tool to view the strategic challenges with homeland security risk management and to provide perspective on how collaboration can improve the existing condition. The book, *The Art of Quantum Planning: Lessons from Quantum Physics for Breakthrough Strategy, Innovation, and Leadership* translates well to the analytic world of intelligence and risk management. The strategic thought and planning literature reviewed for this thesis comports with the literature on collaboration.

THIS PAGE INTENTIONALLY LEFT BLANK

II. HOMELAND SECURITY RISK MANAGEMENT AND ANALYSIS

This chapter provides an overview and assessment of the Risk Analysis and Management structure as it currently exists within the homeland security enterprise. The first section within the chapter introduces the concept of risk management as it applies to the homeland security enterprise. Section B provides an overview of the risk management framework that currently exists within the homeland security enterprise. The tools and strategies common to the framework were developed by components within the U.S. Department of Homeland Security with the intent that they would be used by the agencies of federal, state, local government, and the private sector to manage the myriad of risks inherent to the homeland security enterprise. The wide spectrum of risk that must be considered within the construct of homeland security make the risk management landscape exceptionally complex.

The third section, Section C, of this chapter explores the significant challenges presented by the different risks considered within the homeland security enterprise. Understanding these obstacles establishes the frame of reference for the reader to understand the argument for establishing a common national framework for homeland security risk management presented in Section D. This section provides a comparison of several risk management models, and it provides an analysis of the strengths and weaknesses of each with the intent of identifying approaches to strengthen the risk analysis and management culture among all partner organizations involved in homeland security.

Sections E and F explore the concepts of enterprise risk management and comparative risk assessment respectively. These concepts provide some insight into possible methods to overcome the obstacles inherent to a common risk management framework within the homeland security enterprise.

A. RISK ANALYSIS AND MANAGEMENT

The concept and practice of risk management resides at the center of the homeland security discipline. Every aspect of homeland security and emergency management programs can be derived from a series of basic problems or questions. These include: *What hazards or threats exist? What are the undesirable outcomes from the occurrence of these events? What are the negative consequences of these outcomes? What can be done to avoid or reduce the negative consequences of these events?* Within this context, every homeland security action, initiative, and program at every level of government is a component of an intricate risk management system. The importance of risk management to the homeland security enterprise is best summarized in this statement from the Quadrennial Homeland Security Review Report: "Ultimately, homeland security is about effectively managing risks to the Nation's security." (United States. Department of Homeland Security, 2010).

The concept of risk used for discussion in this thesis comes from the 2010 *DHS Risk Lexicon,* where risk is described as, "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences." (United States. Department of Homeland Security (DHS), 2010 p. 27). The conceptual framework employed by DHS for risk analysis describes risk as a function of threat or hazard (*T/H),* probability (*P),* and consequence (*C*) or *R=((T/H)(P)(C))* (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 2). It is important to remember the importance of time as a frame as we consider risk management, as it significantly influences our perception of threat or hazard and probability of occurrence. People and organizations tend to base risk management decisions on both empirical data and emotion. Most people and organizations have difficulty with understanding numbers, consequently they often perceive the probability of risk based on their ability to readily recall similar events for comparison and perception of risk compared to value gained (Ropeik, 2010).

Several variations of a definition for *risk management* exist within the homeland security framework. The Department of Homeland Security's *DHS Risk Lexicon* defines risk management as, "the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken." (United States. Department of Homeland Security (DHS), 2010 p. 30). The *Baseline Capabilities for State and Major Urban Area Fusion Centers* describes risk management as, "Risk management is a continual process or cycle in which risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and avoidance." (United States. Department of Homeland Security, 2008 p. 53). The *Target Capabilities List*, another publication from the U.S. Department of Homeland Security, uses a definition for risk management provided by the Government Accountability Office (GAO), "A continuous process of managing—through a series of mitigating actions that permeate an entity's activities—the likelihood of an adverse event and its negative impact."(United States. Department of Homeland Security, 2007 p. 43).

While similarities exist among these examples, the differences point out that risk management is a complex issue that remains difficult to coordinate across the enterprise. Ideally, a single definition would assist with coordinating efforts. The scope of risk analysis within the homeland security enterprise is expansive requiring a wide range of subject matter expertise and many different approaches and models tailored to a specific application. Risk analysis is the, "systematic examination of the components and characteristics of risk" (United States. Department of Homeland Security (DHS), 2010 pp. 27–28). This analytical process defines risk components, so that they can be understood and subsequently managed. In some cases, elements and organizations within the U.S. Department of Homeland Security are entirely responsible for risk analysis and management. However, this is not the case for the majority of risks associated with the homeland security enterprise. For the majority of homeland security risks, the

responsibility for analysis and management is spread among multiple organizations at all tiers of government and the private sector (United States Department of Homeland Security (DHS), 2011).

The challenges for coordinating risk analysis and management extend beyond the differences among the missions and focus of various agencies to include the needs for strategic, operational, and tactical decision making within these agencies. A report from the Homeland Security Institute identifies these tiers as mission-based system definition, system-based risk assessment, and risk informed decision making (Cummings, McGarvey, & Vinch, 2006). The nuances of these tiers will be described in the next section that describes the nature of the existing homeland security risk assessment and management framework.

B. THE HOMELAND SECURITY RISK ANALYSIS AND MANAGEMENT FRAMEWORK

No single unified risk analysis framework exists within the homeland security enterprise. The underlying reason for this reality is that the risks within the homeland security domain are too numerous and multi-dimensional with their own unique attributes (Cummings, McGarvey, & Vinch, 2006). Some risk management experts from both public and private sector organizations believe DHS should construct a single integrated approach to risk analysis and management (Government Accountability Office (GAO), 2008). However, the diversity of risks, multiple risk analysis models, and different missions create a formidable challenge that demands strong collaboration. The 2006 report from the Homeland Security Institute supports this conclusion with findings that risk analysis within the homeland security environment is exceptionally complex, requiring significant diversity of expertise, and that noncollaborative processes can lead to an unbalanced approach to risk management, which can produce unacceptable residual risk and risk shifting without increasing security Cummings, (McGarvey, & Vinch, 2006). This problem forces us to consider, *how to combine these elements into a single approach that has utility at each level of government and the private sector?*

The volume and diversity of threats and hazards considered within the homeland security risk management framework present several inequities and challenges that are important for understanding the problems associated with analysis. While the risk analysis responsibilities for U.S. Department of Homeland Security include natural hazards, terrorism, public health threats, and infrastructure failure, these efforts are substantially weighted to focus on terrorism risk analysis (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). It remains unclear if this bias results from public reaction to terrorism acts and political pressure, or if it is the result of a more thorough understanding and sophistication of modeling risks associated with natural hazards and threats to public health. The asymmetric nature of terrorism increases the level of uncertainty. Terrorism also represents a catastrophic risk as opposed to a chronic risk like flooding, and the graphic media coverage following attacks making it an easy risk to recall from our memory (Ropeik, 2010 pp. 105–114). These factors influence emotional responses to risk that can override empirical based judgments, thus, increasing the perceived risk from terrorism (Ropeik, 2010). The emphasis on terrorism risk analysis and management can also be seen in the allocation of homeland security funding. Population density, economic index, and threat assessment clustered in urban areas provide the basis for “risk” in the distribution of homeland security funds (Government Accountability Office (GAO), 2008b).

The assessment of risk from natural hazards is the most evolved due to the foundation of high-quality data sets and refined models. This component of risk analysis also benefits from long-term inter-agency coordination and collaboration in understanding and modeling natural hazard risk, which is evident in reviewing the various models, reports, and state and local hazard mitigation plans that routinely cite input and expertise from the Federal Emergency Management Agency (FEMA), U.S. Army Corps of Engineers (USACE), the National Weather Service (NWS), U.S. Geological Survey (USGS), and many other relevant organizations. Since the implementation of the Disaster Mitigation Act (DMA) of 2000, state and local governments have made significant improvements to their natural hazard risk assessments and management strategies. It is important to note that this hazard mitigation

planning effort often does not include terrorism or man-made hazards. This can be seen in a 2009 analysis of state hazard mitigation plans that examined 30 plans for costal states, which are also those with the greatest populations. This analysis shows that only 50% of the plans reviewed address man-made hazards that include terrorism (Berke, P, Smith, G, and Lyles, W, 2009).

Even with the sophistication of the risk analysis associated with natural hazards, significant improvement is needed to support long-term risk management and policy decisions with emphasis in three specific areas. The areas requiring significant improvement include developing a better understanding of the social aspects of risk, efforts to support local and regional risk-based decision making, and understanding infrastructure independencies as to avoid cascading failures (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). This deficiency in the collective understanding of the social aspects and cascading interdependencies among complex networks is a challenge that transcends both terrorism and natural hazard risk assessment programs throughout the homeland security domain.

The risk associated with terrorism remains hard to model because of the large inconsistency among independent variables. Data limitations make it nearly impossible to characterize threats and consequences, and the second order social and economic effects of terrorism have been largely overlooked so far in accounting for the risk from terrorism (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 pp. 46–51). Another significant consideration in analyzing the risk associated with terrorism is that threat, vulnerability, and consequence are interdependent variables instead of independent variables, which significantly increases the difficulty in drawing conclusions from the analysis (Cox Jr., Louis Anthony (Tony), 2008). This concept can be illustrated with an intelligent adversary with any number of motivations that is able to change targets and adapt tactics based on experience and observation of countermeasures. The reality of these challenges forces the Department of Homeland Security (DHS) and other entities involved in the homeland security enterprise to rely on expert judgment, which is difficult to reproduce and is very subjective, for terrorism risk analysis. DHS recognizes that risk assessment for terrorism is a complex process that

requires multiple types of expertise to be effective, and that noncollaborative approaches to risk management often leave unacceptable residual risk (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

Three broad approaches to conducting terrorism risk assessment can be identified, with each method offering strengths and shortfalls: expert opinions, simulations, and historical data analysis (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 49). Expert opinion provides a rapid qualitative assessment from a variety of technical experts and intelligence analysts. It also offers an analysis where empirical data cannot be obtained due to technical, technological, resource, or ethical limitations; however, it does not provide a substitute for data collection and analysis (Cummings, McGarvey, & Vinch, 2006b). Another notable shortfall of expert opinion is the potential for individual or organizational bias, and limitations of expert knowledge. Simulations include a wide range of methodologies to include physical, analytical, and engineering simulations. These include computer models, fault trees, red teaming, and game theory approaches, to name a few. While simulations provide a more structured and empirical approach to risk assessment, they require significant amounts of high quality data, time, and technical expertise to produce results, and may be limited by available technology. The collection and analysis of historical data also provides an avenue for evaluating terrorism targeting and methodologies. However, it is generally limited by sparse data sets and the past events for which data is available are situation specific, and so it is difficult to draw any general risk conclusions with any degree of validity (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 50).

The vulnerability and consequence analysis components of terrorism risk assessment also present significant challenges. Both vulnerability and consequence analysis tend to rely heavily on expert opinion and judgment. The vulnerability analysis component of risk analysis in the homeland security environment tends to be focused heavily on physical security (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 51) . This emphasis in one area can lead to errors of omission where other vulnerabilities are not identified, leaving some risks

unaccounted for. Consequence analysis related to terrorism risk also proves difficult because the intangible and secondary effects are hard to quantify. In some cases, secondary effects, such as long-term economic impact, business interruption, psychological and societal impacts are not always adequately modeled; however, the consequences can be magnified as a result of terrorism events (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p.51).

The existing homeland security risk analysis and management landscape is complex involving many different risk assessment models to support tactical, operational and strategic decision making across a multitude of missions. This complex framework is described as having three tiers that include; mission-based system definition, system-based risk assessment, and risk informed decision making (Cummings, McGarvey, & Vinch, 2006a). Tier I is *Mission-Based System Definition,* defines the scope through objectives and system boundaries. This tier focuses on assessing threats and risks to systems and relating these assessments to mission and security/protection goals and objectives. These assessments often involve scenario based assessments, which aid in tactical decision making and provide input to the next level of assessment. Tier II is *System-Based Risk Assessment,* which includes the identification and analysis of threats, vulnerabilities, and consequences. This tier advances the assessment beyond the risk and vulnerabilities to the component parts and begins to account for second and third order impacts to larger systems. And Tier III is *Risk Informed Decision Making,* in which policy makers and senior executives make decisions based on information from Tiers I and II (Cummings, McGarvey, & Vinch, 2006a).

Risk communication is another significant component of the three tier model because it transcends all three tiers in the framework enabling discourse among multiple disciplines and organizations involved at each level. The discourse associated with risk communication is important because stakeholder organizations have different perceptions of risk and tolerance levels (Cummings, McGarvey, & Vinch, 2006a). This three tiered organizational framework provides a methodical approach to scope, assess, and communicate risk so that it can be factored into decision making at each tier of government. The twenty-five methods, techniques, and tools for risk assessment

described and analyzed in Volume II of the Homeland Security Institute report are focused on terrorism and infrastructure protection, which is reflected in Cummings, McGarvey, and Vinch's discussion of the three tiered model. The three tiered risk assessment model provides a useful frame to consider the dynamics and relationships intrinsic to risk analysis and management within the homeland security enterprise. The exchange of information and discourse supported by risk communication highlight the opportunity for greater collaboration. The differences between the various risks, assessment models/strategies, and missions within the enterprise present significant challenges to be explored in the next section of this chapter.

C. CRITICAL CHALLENGES FACING HOMELAND SECURITY RISK MANAGEMENT

Significant challenges present themselves as we consider applying risk management principles across the homeland security enterprise. Two reports, one published by the Government Accounting Office (GAO) in 2008, *Strengthening the Use of Risk Management Principles in Homeland Security*, and the other published by the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*, capture these significant challenges. Generally speaking, these challenges are grouped into political obstacles, failures in strategic thinking, partnership and coordination challenges, the lack of a strong understanding of risk management practices, and risk communication challenges.

Given multiple tiers of influence from elected officials, the political challenges facing risk assessment and management within the homeland security domain are varied. In this context, grants authorized by Congress and delivered to state and local government through the Department of Homeland Security (DHS) provide the greatest leverage over state and local government (Masse, T, Rollins, J, & O'Neil, S, 2007). This leverage is viewed as an important tool to secure the cooperation of state and local government in achieving federally driven goals and objectives. The President's National Strategy for Homeland Security suggests an emphasis on risk assessment to meet homeland security goals (Buschmann, 2002). This implies the importance of risk assessment in setting and achieving national level homeland security goals. The desire of

politicians to deliver goods and services to their constituents in the form of earmarks and special projects, often works against projects that provide long-term trade-offs and changes in risk perception over time (Government Accountability Office (GAO), 2008a). This manifests in a reluctance to incur up-front risk management costs in return for a reduction in risk that may not be fully realized until some years later. Additionally, public perception of a risk is heightened following a significant occurrence, which also provides political incentive to take action that the public views as having immediate impact on the risk. This phenomenon is related to a number of factors, such as ease of recall, control, uncertainty, and fairness among others that influence the emotional aspect of risk perception (Ropeik, 2010). These significant challenges of viewing risk strategically will require time and the attention from leadership to resolve. To accomplish this, DHS needs to look beyond the assessment of risk to the integration or risk into the establishment of goals and objectives associated with programmatic and budget cycles (Jenkins, 2007).

The lack of strategic thought related to risk management within the homeland security discipline goes beyond program and budget cycles. The absence of public discourse on homeland security risks significantly contributes to the shortfalls in strategic thought. The dialog on risk management should include all stakeholders, which include the public, private sector, federal agencies, and state, local, and tribal governments. This discourse is important to evaluate the trade-off decisions expected of political and executive leadership. Nontechnical considerations derived from public discourse can balance technical assessments and limit the effectiveness of technical assessments if not accounted for (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 23). The unique responsibilities of government emphasize the downside of risk mitigation, preparedness, response and recovery, but each challenge can also provide a business opportunity to the private sector to design technology and measures to improve resiliency (Government Accountability Office (GAO), 2008a). Risk management must also balance a wide array of risks ranging from terrorism to natural hazards, and infrastructure failure across the homeland security enterprise. The diversity

of risk perception among the various homeland security stakeholders emphasizes the need for discourse and a symbiotic partnership between government and the private sector.

Perhaps the most important group of risk management challenges for homeland security relate to coordination and partnerships. The totality of homeland security risks need to be viewed as an amalgamation of private and public sector issues in lieu of being seen as only a government centric problem (Government Accountability Office (GAO), 2008a). The lack of intergovernmental partnerships and public private sector partnerships for risk management remains a challenge that was also identified in the *Recommendations for a National Mitigation Effort*, published by NEMA in 2009. Risk management efforts within the federal government, and even within the Department of Homeland Security, remain largely fragmented (Jenkins, 2007). Although DHS recently published a homeland security risk management doctrine, current risk management guidance remains insufficient. This is largely due to the fact there is great disparity among agencies at all levels of government with respect to maturity, understanding, and application of risk management concepts and principles (Government Accountability Office (GAO), 2008a). Finally, even with acknowledging the existence of the DHS Office of Risk Management and Analysis, all of the reports reviewed agree that coordination is handicapped due to the absence of a single point of contact, such as a risk management officer or office to coordinate risk management efforts throughout the homeland security discipline. Although the reports agree on this point, they differ on how best to address this issue. The implementation of the principle of “transparency” as described in the homeland security risk management remains important to improving collaboration and partnerships for risk management.

The challenge of educating homeland security stakeholders in risk management concepts and principles must be overcome to facilitate greater collaboration and partnerships, overcome political obstacles, and improve strategic thinking. The separation and analysis differences between the risk management and intelligence functions within the homeland security enterprise significantly contribute to the shortfalls in collaboration between these disciplines. Intelligence analysis often supports the larger risk management

mission, but there is a general lack of appreciation for rationales, responsibilities, and methodologies of risk assessment within the intelligence community (Government Accountability Office (GAO), 2008a). Although the processes and focus between the intelligence and risk analysis community disciplines may differ, both offer analysis important to the risk management process. Training intelligence analysts in the risk analysis and management concepts and principles could help improve coordination and collaboration between these disciplines. The federal government has fallen short on educating state and local government in risk management concepts and principles as they relate to homeland security (Government Accountability Office (GAO), 2008a). This oversight creates significant problems, since the federal government asks state and local governments to spend money in accordance with national priorities and initiatives. The Department of Homeland Security recognizes this shortfall, and seeks to incorporate more state and local input into risk analysis and risk management decisions (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 59). Improvement to risk management education among all stakeholders in the homeland security enterprise is a critical aspect of enabling the “unity of effort” identified as a key principle in the homeland security doctrine.

The complications related to homeland security risk communication are largely the sum of the obstacles from the other groupings. Although DHS published the *DHS Risk Lexicon* in 2007 with an update in 2010, the document is not widely known or used by all partners in the homeland security risk management community. When I shared the document with the State Hazard Mitigation Officers over our informal collaboration network, the vast majority had never seen the document, and communicated that their agencies were not using the document. I encountered similar results when I shared the document with the public health community within the State of Idaho. The overt focus on unlikely risks with dramatic consequences creates a condition where public fear undermines efforts to engage in a fact-based analysis of risk (Government Accountability Office (GAO), 2008a). All of the reports reviewed also agree that the limited consideration of behavioral impacts present a significant shortfall in risk analysis and management efforts. The improvement of behavioral, psychological, and sociological

aspects of risk emerges as a key theme from the report, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

Examination of existing risk analysis and management practices within the homeland security enterprise reveals several efforts to encourage collaboration and produce a common strategic vision for risk management; however, the shortfalls overshadow these efforts. Effective collaboration for the management of homeland security risk requires leadership, guidance, and the involvement of all stakeholders. The next section explores the need for this common framework.

D. NEEDED: A COMMON NATIONAL FRAMEWORK FOR HOMELAND SECURITY RISK MANAGEMENT

Since the creation of the Department of Homeland Security in 2002, multiple organizations, reports, and studies have called for a coordinated national strategy for homeland security risk management. FEMA's *2006 Nationwide Plan Review: A Report to Congress* identified a need for national guidance on catastrophic risk analysis. A white paper published by the National Emergency Management Association (NEMA) in 2009 called for the development of an effective national mitigation effort, and to accomplish this, it identifies the three strategic themes that include broader collaborative partnerships, total hazard awareness, and full spectrum community-to-federal emphasis (National Emergency Management Association, 2009). These themes present a framework for a reexamination of the way in which we assess and analyze risk, and the manner in which we prioritize the functions of risk analysis, mitigation/prevention, and preparedness. The *2010 Nationwide Plan Review* identifies the need for a risk assessment and management process usable by all levels of government (Federal Emergency Management Agency (FEMA), 2010). Additionally, the *Quadrennial Homeland Security Review Report* emphasizes the need to collaboratively analyze homeland security risks in order to manage them effectively at every level of government and the private sector (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

The need for a more effective and standardized national approach for homeland security risk analysis and management is clear, and supported at each level of government. This leaves us with the question, *what has been done thus far to develop national risk analysis and management process*? The Department of Homeland Security created the *DHS Risk Lexicon* in 2008 to establish a common vocabulary for risk analysis and management across the homeland security enterprise. A revised version of this document was released in September 2010. The National Mitigation Alliance was created in 2011 to foster a collaborative process to reach across disciplines and levels of government to promote a comprehensive national mitigation framework. The National Mitigation Alliance is the product of a cooperative agreement between FEMA and the National Emergency Management Association to implement the vision outlined in the NEMA white paper. The alliance provides a collaborative model that addresses risk management through strategic themes to include total hazard awareness and full-spectrum community-to-federal emphasis (National Emergency Management Association, 2009). Additionally, DHS published *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* in April of 2011. This document is intended to serve as, "an authoritative statement regarding the principles and process of homeland security risk management and what they mean to homeland security planning and execution" (United States Department of Homeland Security (DHS), 2011). Although not the complete solution, this document provides an important piece in creating a culture of risk management within the homeland security environment.

State and local governments need to play a larger and more active role in homeland security risk management. DHS acknowledges the need to include more state and local input into its risk assessments (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 p. 59). Evidence of this realization can be seen in the Emergency Management Performance Grant (EMPG) and Homeland Security Grant Program (HSGP) Guidance documents for federal fiscal year 2011. Both of these documents list objectives for states to develop Threat and Hazard Identification and Risk Assessments (THIRA) to include the entire range of threats and hazards faced by the respective jurisdictions. The guidance goes on to communicate the importance of

including terrorism and other man-caused hazards into the state hazard mitigation plans that have been developed by the states. As of the publication of this paper, no specific guidance or job aids have been issued to state and local governments on a standard methodology for developing a THIRA.

Multiple risk management models and standards exist within the homeland security enterprise. The following chart provides a comparison of risk management guidelines from several documents familiar to the emergency management and homeland security communities. These documents provide recognized industry standards and common capabilities. The documents compared include the DHS Target Capabilities List, National Fire Protection Association Standard 1600 (All-Hazards Emergency Management/Homeland Security), Emergency Management Accreditation Program (EMAP), FEMA Guidelines for State and Local Hazard Mitigation Plans, and DHS State and Major Urban Area Fusion Center Capabilities. Examination of the similarities and differences between these documents can help us improve coordination among agencies to improve risk management throughout the enterprise.

Table 1. Comparison of Guidelines and Standards with Risk Analysis and Risk Management Attributes

Comparison of Guidelines and Standards With Risk Analysis and Risk Management Attributes Within the Homeland Security Framework								
Emergency Management / Homeland Security Guidance and Standards		**Risk Management Attributes**						
		Develop a Risk Management Framework	Assess Risks	Prioritize Risks	Develop a Business Case	Manage Risks	Risk Communication	Includes Intelligence
	Target Capabilities List (2007)	X	X	X	X	X	X	X
	National Fire Protection Association Standard 1600		X	X	X	X		
	Emergency Management Accreditation Program (EMAP)		X	X	X	X	X	
	FEMA Guidance for State and Local All-Hazard Mitigation Plans		X	X	X	X	X	
	Baseline Capabilities for State and Major Urban Area Fusion Centers		X				X	X
	Fusion Centers Critical Infrastructure / Key Resources Protection Capabilities	X	X				X	X

Examination of the various guidance and standard documents and their associated attributes compared in Table 1 provides insight into the strengths of homeland security risk management. The assessment and communication of risk are the most common attributes between the various documents compared. These two common elements provide an opportunity to open a dialog and draw the terrorism centric homeland security risk assessment/management community and the natural hazards centric emergency management risk assessment/management community closer together.

Analysis of the various guidance and standard documents and their associated attributes in Table 1 also identifies key differences that can be viewed as shortfalls in

some of the approaches reviewed. The three emergency management focused standards do not include intelligence as an attribute. This is likely due to the fact that the inclusion of man-made hazards, which include terrorism, are not encouraged in state and local hazard mitigation plans (Federal Emergency Management Agency (FEMA), 2007 p. 59). The two fusion center capability documents do not include attributes associated with the prioritization of risks, development of a business case, or the management of risk. This could be due to the challenges with assigning probabilities and empirical models to the asymmetric threat of terrorism or the separation of intelligence and risk analysis within the homeland security enterprise. The inclusion of risk prioritization, business case development, and risk management in the emergency management centric standards is likely due to the experience with natural hazard mitigation planning. Integrating the natural hazards program experience with building business cases and prioritizing risks could advance efforts to implement a comprehensive approach to risk management within the homeland security enterprise as recommended by the GAO (Jenkins, 2007).

E. ENTERPRISE RISK MANAGEMENT

This section discusses enterprise risk management and compares several risk management models. The concepts of enterprise risk management and integrated risk management are closely related in the homeland security context. Enterprise risk management is defined as a, “comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization’s ability to achieve its objectives” and integrated risk management is defined as a “structured approach that enables the distribution and employment of shared risk information and analysis and the synchronization of independent yet complementary risk management strategies to unify efforts across the enterprise” (United States. Department of Homeland Security (DHS), 2010 pp. 12–13, 19). Both concepts emphasize the importance of sharing information to synchronize independent systems and organizations for effective risk management across the enterprise.

The DHS Risk Management Doctrine incorporates both of these concepts into the national vision for homeland security risk analysis and management (United States

Department of Homeland Security (DHS), 2011). Further evidence of the commitment to an enterprise risk management system comes from the DHS Policy for Integrated Risk Management signed by Secretary Napolitano in 2010. The policy stipulates achieving integrated risk management by incorporating the risk management process into the overall mission of DHS encompassing all subcomponent organizations, using risk information to achieve greater degrees of transparency and risk-informed decision making, and using a unified approach to manage risks with all partners involved in the homeland security venture (Kolasky, 2011).

The International Organization for Standardization (ISO) recently published ISO 31000:2009 Risk Management Principles and Guidelines as a standard that would apply internationally to all forms of risk. The diversity of risk, complex challenges, and need for system adaptability to address contextual issues and emerging risk required for the ISO 3100:2009 standard directly compare with those issues faced by enterprise risk management within the homeland security discipline. Not surprisingly, many similarities exist between the ISO 3100:2009 standard, the approach laid out by the U.S. Department of Homeland Security. Several key differences in these models are also noteworthy. This standard has received the attention of the emergency management and homeland security community as a significant advance in emergency management concept for the comprehensive management of disaster risk at the community level (Jones, 2011 (May)).

The expansive scopes of the ISO risk management standard and the risk management approach within the homeland security enterprise both require a common vocabulary to transport information and concepts across different domains. The homeland security model includes the DHS Risk Lexicon for this purpose while the ISO 31000:2009 standard provides terms and definitions in clause 2 and makes reference to a glossary of risk management terms, ISO Guide 73:200. The importance of clearly defined common terminology cannot be overlooked when working with the wide range of partner organizations working towards the common goals of resiliency and security, as we have in the homeland security enterprise. The homeland security community should avoid the shortfalls from the ISO 31000 approach to a common vocabulary. These shortfalls include ambiguous definitions that often use words that express generalities in lieu of

specifics, a general avoidance of mathematical words, and the assignment of new interpretations to terms already widely used and accepted within the risk community (Leitch, 2010). The DHS Risk Lexicon avoids this pitfall so far; however, future iterations will also need to include the same precision with definitions.

Performance measurement provides another common thread between the ISO standard and the homeland security system for risk management. The ISO standard provides a more general discussion of performance criteria; however it does identify several key principals that easily apply within the homeland security context. These guiding principles for risk management include: 1. Effort should create and protect value, 2. Be a significant part of decision making, 3. Explicitly address uncertainty, 4. Include a systematic, structured and timely process, 5. Be based on the best available information, 6. Be tailored to the specific context, and 7. Facilitate continual improvement to the organization (Purdy, 2010). The guidance offered by DHS is also general in nature, although it does provide more detail in methodologies. It includes the use of logic models that incorporate goals, inputs, efforts, outputs, and outcome performance measures.

The homeland security model also emphasizes the role of red teaming (scenario role-playing), exercises, surveys, and unbiased external review. DHS describes the best measure for risk management performance as either the continued appropriateness of risk acceptance or the reduction of the likelihood or consequences of a risk (United States Department of Homeland Security (DHS), 2011). This supports the concept strategic planning through scenarios as described by Van der Heijden in the book, *Scenarios*.

One curious omission from the discussion on performance measurement in both approaches is the role of the cost-benefit analysis modeling and subsequent loss avoidance studies. Both cost-benefit analysis models and loss avoidance studies figure prominently into the FEMA risk management programs for natural hazards. A cost-benefit analysis is an important factor in making a business case, which is identified as an important attribute in most of the guidance and standards documents reviewed (Federal Emergency Management Agency (FEMA), 2003).

A clearly defined process lies at the heart of all risk management systems, and neither of the DHS or ISO approaches are an exception to this rule. Each of their respective risk management processes, shown in Figures 1 and 2, contain some common elements that include establishing a context, identification and analysis of risk, communication, and the evaluation and monitoring feedback loop. The DHS process model shown in Figure 1 includes the development of alternatives and decision and implementation. These steps or an equivalent are conspicuously missing from the ISO model shown in Figure 2. The ISO standard emphasizes the importance of including the risk management process in decision making, but it neglects to include the decision-making steps in the process model. This noteworthy omission from the ISO model should caution state and local emergency management organizations from adopting the ISO model at face value without evaluating other models. The development of alternatives and decision/implementation steps are critical for engaging leadership in a discourse to consider all viable risk management strategies for emergency management and homeland security risk management issues.

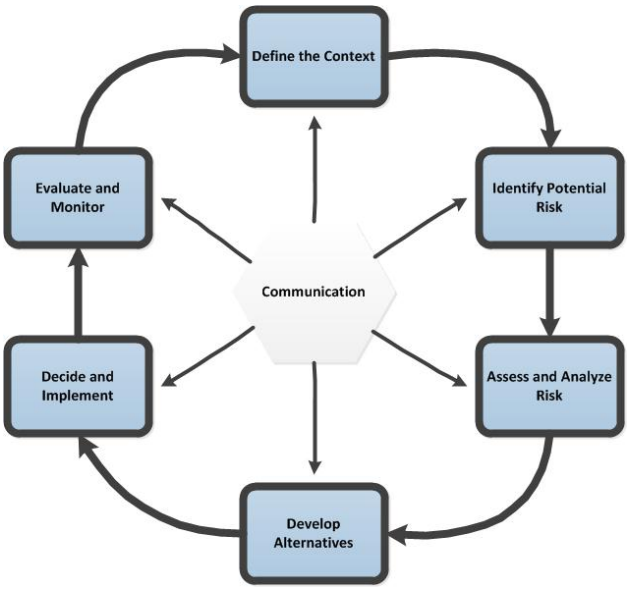

Figure 1. DHS Risk Management Process from (United States Department of Homeland Security (DHS), 2011 p. 15)

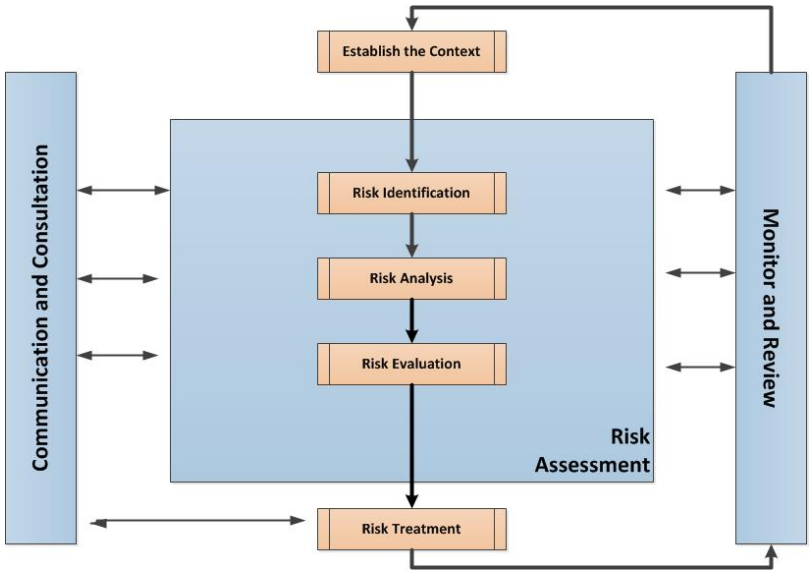

Figure 2. ISO Risk Management Process from (Purdy, 2010)

Both the ISO and DHS risk management models agree that the risk management process should be incorporated into the organizational decision-making process. Both models also agree that the concepts within their respective risk management process models should be tailored to address the situation and perspectives of the organizations applying them. The importance of scalability and adaptability with these process models in the homeland security context is evident considering that an enterprise wide model must work for multiple tiers of government agencies with different missions, the private sector, and nonprofit volunteer organizations.

Another risk management model important to the homeland enterprise is the Risk Management Framework located within the National Infrastructure Protection Plan (NIPP) published in 2009, which is depicted in Figure 3. The 2009 update to the NIPP includes greater emphasis on risk management and resilience. This includes significant updates to risk methodologies and information sharing systems (*Critical Infrastructure Protection Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience.* 2010). A comparison of the NIPP Risk Management Framework to the common elements of the DHS and ISO risk management models reveals some awkward connection in terms of vernacular and process. The first two steps

of the NIPP framework include setting goals and objectives and identifying assets, systems and networks. These steps are similar to the step for establishing context in the DHS and ISO models. The NIPP does not include an evaluation of alternatives unless this is included in the prioritization step, while this is built into the DHS model.

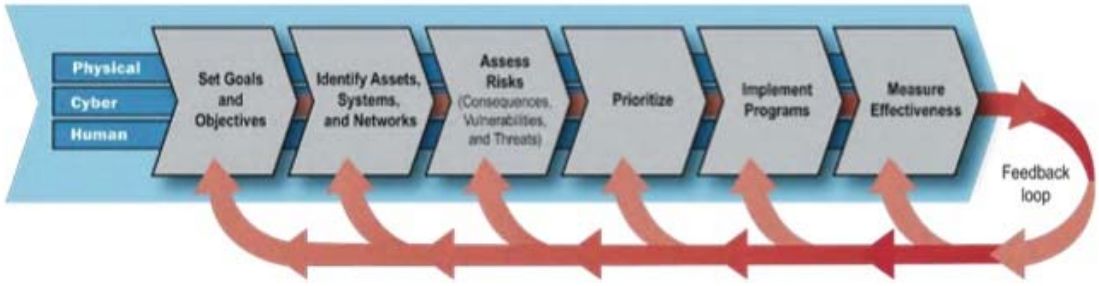

Figure 3. National Infrastructure Protection Plan Risk Management from (*National Infrastructure Protection Plan.* 2009)

The greatest drawback to the NIPP Risk Management Framework is the difference in terminology compared to both the DHS risk management model and the ISO model. The success of the infrastructure protection program relies heavily on partnership with private industry and state and regional fusion centers to collect, analyze and share information (*National Infrastructure Protection Plan*2009). The private sector partners are more likely to use and be more familiar with the ISO model as industry standards, which are more similar to the DHS model than the NIPP model. Additionally, the use of different models for the same concept within the homeland security enterprise makes communication and collaboration more challenging.

F. COMPARATIVE RISK ANALYSIS

The concept of comparative risk analysis provides a framework that can be used to compare many different risks within the homeland security enterprise. The U.S. Environmental Protection Agency pioneered comparative risk ranking with the publication of *Unfinished Business: A Comparative Assessment of Environmental Problems* in 1986. This comparative risk analysis process involves categorizing risks and identifying key attributes to serve as the basis for comparison (U.S. Environmental Protection Agency (USEPA), 1987). This innovative approach to risk ranking allowed

experts and lay people to engage in a dialog to collectively rank the risks (Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B., Fischbeck, P. S., & DeKay, M. L., 2001). The adaptability of the comparative risk assessment approach makes it useful for decision making across a wide spectrum of risk issues while allowing for the combination of emotional, social, and political issues and facts backed with empirical data to support decision making (Power & McCarty, 2006). This innovative approach was not without its problems. The key deficiencies with the EPA study conducted in 1986 relate to the categorization of the risks considered. Confusion over the categorization of risks resulted from an inconsistent approach where some environmental risks were categorized by source, some were categorized by the physical agent responsible for harm, and still others were categorized by accidental or routine occurrence (Morgan, Florig, DeKay, & Fischbeck, 2000).

The Carnegie Mellon Risk Ranking Method consists of five steps as shown in Figure 4. It provides the basis for comparative approach to risk assessment. This process is described by Florig et al. (Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B., Fischbeck, P. S., & DeKay, M L., 2001) and Morgan et al. (Morgan et al., 2000). The first step involves defining and categorizing the risks to be evaluated and ranked. The step identifies which attributes for the risks should consider in the comparison. These two steps are most often done together so that the list of categories and attributes to be considered evolve together. The risks are then summarized on summary sheets or reports for comparison. Next, participants are selected and a comparative analysis is performed to produce the risk rankings. Finally, the issues associated with the key issues being described to support the final rankings. Value judgments and perspective of those involved figure significantly into each step of the process.

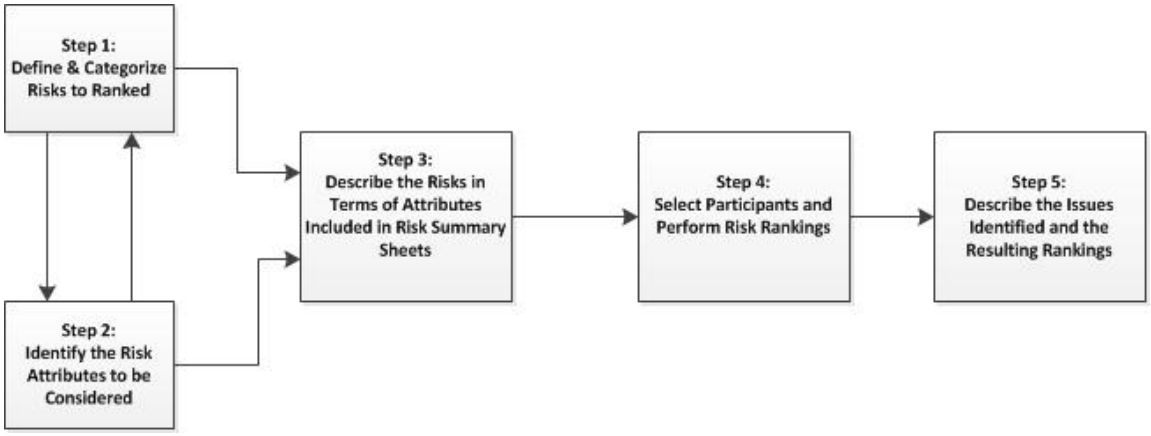

Figure 4. Carnegie Mellon Risk Ranking Method from (Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B.,Fischbeck, P. S.,& DeKay, M. L., 2001)

The success of a comparative approach to risk assessment and ranking depends largely on how the comparisons are framed for the decision makers and stakeholders charged with risk management. The division and categorization of risks provides the basis for establishing the frame of comparison, and thus the results of risk ranking endeavors are subject to influence from this initial step (Morgan et al., 2000). Most risk ranking efforts have invested too little attention to framing and facilitating the ranking, and thus stifling risk communication and discourse among stakeholders (Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B., Fischbeck, P. S., & DeKay, M. L., 2001). Value judgments also factor significantly into several aspects of comparative risk assessment. Obviously, value judgments figure significantly into objective comparison of which two hazards or threats are inherently more risky. Additionally, the relative importance of attributes and categorization of risks require value judgments that ultimately influence the frame of the assessment (Morgan et al., 2000).

G. OBSERVATIONS AND CONCLUSIONS

Numerous standards and ideas about risk management exist among government and the private sector alike. The homeland security domain is expansive and requires an adaptive framework that can fuse the best of these elements together instead of trying to construct a one-size fits all risk assessment and management tool. The risk management framework must incorporate both qualitative and quantitative analyses, common

terminology and guiding principles, and be able to facilitate and manage discourse among many disciplines and stakeholders. Ultimately, it must be a useful tool in supporting decision making within local, state, and federal government and the private sector.

A fully integrated risk analysis approach remains impractical given the wide range of unique risks that must be considered within the homeland security discipline. An integrated risk analysis model requires risks to be compared in a common metric. The quality and availability of data sets available for establishing probability, vulnerability, and consequence for each hazard or threat is too diverse to fit within a common metric, and the level of uncertainty associated with these variables is not consistent for the various hazards and threats (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). The diversity of analysis tools and metrics provide additional detail that is beneficial to decision makers (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). An integrated risk analysis approach would need to be highly quantitative to be effective, and this would limit the benefit that the discourse of qualitative risk analysis adds to discussions and decision making.

Comparative risk assessment and ranking provides an approach that incorporates the strengths of both quantitative and qualitative methods of risk assessment to support decision making. The selection of risk attributes in the Carnegie Mellon Risk Ranking Method allows diverse risks to be compared on an equal footing. DHS should employ a comparative risk assessment tool, as it allows multiple metrics to be compared against common attributes allowing stakeholders and policy makers to incorporate best judgment into the decision-making process (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010, p. 87).

The success of the homeland security enterprise depends largely on accurate and coordinated risk analysis and management, and the complexity and need for collaboration among a multitude of agencies and disciplines demands effective leadership to coordinate these efforts. The lack of a Chief Risk Officer (CRO) is cited as a factor discouraging effective leadership and collaboration (Government Accountability Office (GAO), 2008a). The homeland security CRO would need to work with many agencies and the

private sector to develop an understanding of existing and emerging risks to establish a risk framework that applies scientific knowledge to assess the frequency, vulnerability, and consequence of various risks. They also need to communicate the findings to policy makers and the public to steer risk management decisions and policy (Government Accountability Office (GAO), 2008a).

A compelling argument against establishing a chief risk officer within the homeland security enterprise exists. The basis for this argument is that there is a need to assess risk among many government agencies for a plethora of issues, and each of these assessments depends on agency mission, concerns to be addressed, methodology, and expertise required. The ability to accumulate the required expertise, develop contextual awareness, and maintain proficiency across the entire spectrum of expertise is daunting at best and more likely a failure (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). The direct interactions between analysts and stakeholders are important and make significant contributions to the qualitative analysis and decision making for risk management, and the creation of a CRO within the homeland security enterprise would dilute this exchange. This lesson was learned when the OMB tried unsuccessfully to construct a single risk analysis tool to be used by all agencies across the government (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

The most important revelation from the literature is the development of a strong culture for risk management within the homeland security community. While this simply stated notion sounds intuitive, it will be a long and difficult process. It will require a more thorough understanding of risk tolerance from many perspectives to include all tiers of government, the private sector, and the public, better risk communication practices, stronger collaboration and information sharing practices, and greater strategic thought (Government Accountability Office (GAO), 2008a). This evolution will require a paradigm shift within the homeland security community from one dominated by what we traditionally consider to be focused on preparedness and response to one that emphasizes the more proactive approaches of protection, prevention, and hazard mitigation. The path

to success requires an enterprise wide shift from reacting to past events and anticipating future events, so that we can prepare ourselves accordingly (Government Accountability Office (GAO), 2008a).

The DHS Office of Risk Management and Analysis has made steps towards establishing a risk management culture within the DHS components. These include the publication of the DHS Risk Lexicon, Creation of the Risk Steering Committee, and most recently the publication of the DHS Risk Management Doctrine, *Risk Management Fundamentals.* However, recent hiring and training programs do not appear to be improving the situation, and other examples of government agencies with a strong risk management culture such as the U.S. Environmental Protection Agency (EPA) and the Nuclear Regulatory Commission (NRC) took many years to develop this culture (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). DHS faces a more substantial challenge than the EPA or the NRC for several reasons. These include the scope and variety of risk across the homeland security enterprise, asymmetric threats and intelligent adversaries, and the stakeholder/partner role shared by numerous local, state, and federal agencies, industry, nongovernmental organizations, and a seemingly endless list of professional disciplines and technical experts.

The Quadrennial Homeland Security Review Report (QHSR) identifies the need for a national-level homeland security risk assessment, but it fails to specify and emphasize the important role of state and local governments in developing and implementing a national approach to risk assessment. The QHSR specifies the need to include intelligence assessments and the expertise and information that exists among the various federal departments and agencies (United States. Department of Homeland Security, 2010). While all of the literature reviewed agrees that a feasible approach for a national-level homeland security risk assessment is needed, the systematic and meaningful incorporation of state and local risk information in federal level assessments remains to be seen (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). To date, insufficient engagement and participation of state and local practitioners and experts in applying risk management concepts to the

homeland security enterprise remains a missed opportunity, since significant amount of knowledge and ability represent an untapped resource (Government Accountability Office (GAO), 2008a). DHS acknowledges the need to incorporate the need to include more state and local input into risk assessments, and this is evident with their efforts in several outreach programs, however, much work remains to improve coordination between DHS and the state and local partners.

The homeland security risk analysis and management literature agree that a need to construct strong risk analysis and management capability within the homeland security enterprise exists. A robust risk management culture will need to include a collaborative effort among a variety of experts from each tier of government and the private sector. Stronger two-way partnerships with academic institutions are needed to improve the education and understanding needed to develop the risk management culture within the homeland security enterprise (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

Although the specifics and level of sophistication among risk analysis and management differ greatly among agencies and missions in the homeland security enterprise, many challenges remain. It is clear the scope of risk analysis and management across the homeland security domain is too vast to be effectively handled by any one entity or by the federal government alone. Stronger coordination and collaboration among all of the stakeholders across the various missions and disciplines could provide significant improvement to all aspects of homeland security risk management at each level of government to achieve the results the citizens of the United States deserve and expect.

The important relationship between intelligence and risk assessment may not be overlooked, if you are to truly understand the landscape of homeland security risk management. The qualitative expert assessments from the intelligence community significantly contribute to terrorism risk assessments. The risk analysis community and intelligence community can learn much from each other to improve the management of risk in the homeland security enterprise. These ideas are explored in the next chapter.

III. INTELLIGENCE AND RISK MANAGEMENT

The intelligence and risk analysis functions each play an important role within the homeland security enterprise. While intelligence and risk analysis are not synonymous, much in common exists between them. The common ground between these two independent concepts is based on a common purpose, which is to allow policy makers to make informed decisions.

A clear understanding of the basic principles of both intelligence and risk management provide the basis of comparison between these two independent yet similar disciplines. This chapter builds on the previous chapter, which provided an understanding of the tenets and issues associated with homeland security risk management by introducing the concept of intelligence and describing the similarities and links shared with risk management. The discussion includes an examination of the support intelligence lends to homeland security risk analysis and a comparison of the intelligence and risk management cycles.

The culmination of the comparison between intelligence and risk analysis and management leads to the introduction of Intelligence-Led Risk Management. This concept combines the intelligence cycle with risk management and risk management principles to support tactical, operational, and strategic level decision making within the homeland security mission. It explains how the common ground and differences between intelligence and risk analysis can be leveraged to improve risk management within the homeland security enterprise.

This chapter will explore how the common ground and differences between intelligence and risk analysis can be leveraged to improve risk management within the homeland security enterprise.

A. WHAT IS INTELLIGENCE?

In order to understand the commonalities and differences between intelligence and risk analysis, we should begin by defining and describing what intelligence is. A reasonable definition of intelligence as a working concept for this thesis is borrowed from

Mark Lowenthal. He describes intelligence as “the process by which specific types of information important to national security are requested, collected, analyzed and provided to policy makers; the products of that process, the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.” (Lowenthal, 2009). The first part of this definition—the collection and analysis of information and the communication of that analysis to decision makers—provides our focus for comparing intelligence and risk analysis. The fruits of this concept are the intelligence assessments, which provide important information regarding targets, capabilities, and intent of adversaries that may execute terrorism attacks on the population or infrastructure. On the surface, this information is incorporated as one aspect of the comprehensive risk assessment within the homeland security purview.

Understanding that intelligence represents an analytical process provides the basis from distinguishing it from just being information. In describing the common understanding of the intelligence process, Lowenthal cites a diagram adapted from the Central Intelligence Agency’s Consumer’s Handbook to Intelligence provided in Figure 5 (Lowenthal, 2009). Policy advisors and senior staff determine what information is needed and how best to collect it during the planning and direction phase. The required information is then collected according to the direction provided. Next, the raw data is processed into a format that can be used by the analysts. During the analysis and production step, analysts review the processed data from multiple sources and fuse the information into the reports and assessments needed to advise policy makers on any number of issues related to national security. These reports and assessments are then distributed to the policy makers who need the information, at which point the process repeats itself based on requirements for additional information or changing priorities (2009 national intelligence: A consumer's guide2009).

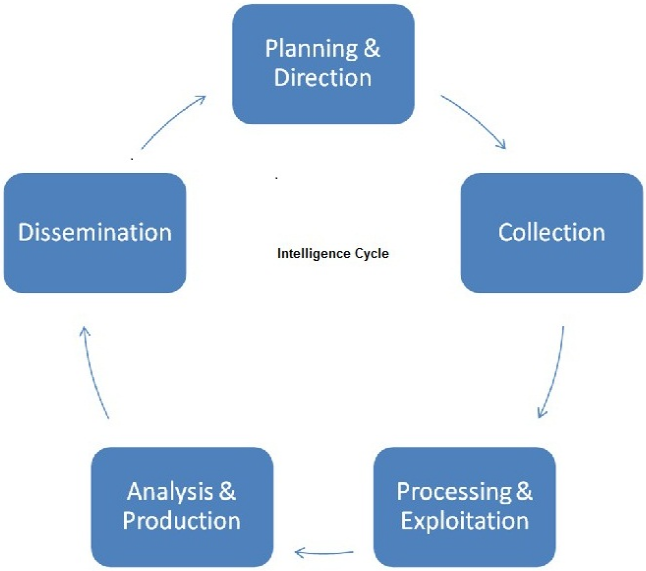

Figure 5. Intelligence Cycle from (Lowenthal, 2009 p. 65)

B. INTELLIGENCE AND RISK ANALYSIS: COMMON THREADS

Information is the currency of both intelligence and risk analysis. Mark Lowenthal asserts, *"All intelligence is information, not all information is intelligence."* (Lowenthal, 2009). The same could be said about risk analysis in that all risk analyses are information, but not all risk information is risk analysis. Simply stated, analysis and added value provide the key distinctions between being just information or the product of intelligence or risk analysis. With this premise, we can explore the similarities and subtle differences between intelligence and risk analysis and determine how the strong points of these elements can work in concert to improve risk management within the homeland security enterprise.

Information provides the lifeblood for the production of intelligence and risk analysis. However, management of the collection and flow of information within both the intelligence cycle and risk management process can present a significant challenge. The volume of information readily available through geospatial intelligence, signals intelligence, human intelligence, measurement and signals intelligence, and open source intelligence provide more data than existing capabilities can analyze. The same holds true

for information sources that provide data for risk analysis. Success of intelligence is not measured by information collected, but instead by the timeliness, efficiency, and, accuracy in supporting decision making (Sims, J. E. & Gerber, B., 2005). The same standard can be applied to risk analysis. Public safety and homeland security organizations need accurate, relevant, timely, and current intelligence to meet their needs for incident mitigation (Townsend et al., 2010). Mark Lowenthal states, "Intelligence is not about truth," and goes on to explain that it is more accurate to think about intelligence as proximate reality (Lowenthal, 2009). This point is important for both intelligence and risk management. In particular, strategic risk management requires analysts to think beyond either/or comparisons and to broaden thought to consider all possibilities, which are tenets of strategic planning (Harris, 2009). The analysis of both intelligence and risk are geared to provide a factual working understanding of a given situation and plausible outcomes based on a number of variable factors.

Both risk analysis and intelligence support risk informed decision making. In each case, policy makers and decision makers require information tailored to their specific needs in order to make informed policy decisions to manage risks. Threat-based foreign policy, global intelligence interests, and consumer-producer relations are recurring themes that shape the U.S. intelligence landscape (Lowenthal, 2009). Intelligence provides information about existing and emerging strategic risks and threats to our national security and interests across the globe. Decision makers use this intelligence information to formulate policy designed to eliminate, minimize, or counter these threats, or in other words, manage these risks. In a similar way, risk analysis provides decision makers with information to formulate policy to manage risk from natural hazards, technological hazards, public health threats, and acts of terrorism. To effectively manage risk to national interests and security abroad, intelligence supports making decisions that enable appropriate action over time (Sims, J. E. & Gerber, B., 2005). This notion of decision-making support, enabling appropriate action over time, and providing information about emerging threats to avoid surprise implies strategic thought. The need for a greater emphasis on strategic thought in homeland security risk management is clear. Risk management experts emphasize the need to improve strategic thinking in the

risk management context, greater use of risk assessments for decision making, and shifting focus from reacting to past events to one of preparing ourselves for those future events that are likely (Government Accountability Office (GAO), 2008).

Both intelligence and risk analysis support the function of providing warning about imminent and emerging threats and hazards to the leaders charged with decision making, and to the public by extension. This common thread to support advance warning allows leaders to evaluate a wider range of options instead of limiting the available options to only the reactive ones. Since the terrorist attacks of 9/11, the call to judge the U.S. Intelligence Community on its ability to provide warning of impending catastrophe has gained significant strength. This ultimately will allow leaders to implement decisions that can prevent or minimize the risk from attacks (Sims, J. E. & Gerber, B., 2005). The risk analysis process supports mitigation and emergency preparedness programs in a similar manner by providing warning about hazards, vulnerabilities, and consequences to decision makers.

Neither intelligence nor risk analysis exist as static processes, and failure to adapt these processes to changes in technology, society, priorities, threats, and the political climate will undoubtedly lead to catastrophe in the future. In general terms, we tend to frame the problems associated with threats and hazards based on our previous experience. Author, David Ropiek, describes the process of how people employ mental short-cuts to make judgments in the absence of perfect knowledge as “bounded rationality.” Bounded rationality involves a number of concepts that factor into how we view issues that are relevant to both intelligence analysis and risk analysis. These include; the idea of categorization or representativeness in which we relate new information to a category familiar to us; the theory of the endowment effect in which the framing of information as a negative or positive connotation changes our perception; the anchoring and adjustment effect in which we derive estimates from making adjustments from a known piece of information; and the ready recall effect in which the more aware we are the easier the information is recalled, and thus the more concerned we are with it (Ropeik, 2010). The bias from the cumulative effects of these concepts can easily influence analysis and produce short-sided intelligence assessments and risk analysis.

Intelligence analysis and risk management exist as dynamic systems that continue to evolve with the collection of information. Intelligence failures occur when the intelligence process does not improve or experiences degradation of capability (Sims, J. E. & Gerber, B., 2005). This problem is characterized by the failure of imagination, policies, capabilities, and management outlined in the 9/11 commission report (Kean & Hamilton, L. H., 2004). Gerald Harris provides a useful description of this process in his book, *"The Art of Quantum Planning."* He describes the quantum change process as a situation when a new event enters a situation or system and affects a change resulting in adaptation and the establishment of a new equilibrium or steady state (Harris, 2009). The terrorist attacks of 9/11 can be seen as such an event to both the intelligence and risk management communities in that the event precipitated change and adaption that resulted in a new system balance of mission, needs, priorities, and stakeholders. Given events with dramatic changes such as this, we must exert effort to preserve existing capabilities, while adapting to new requirements communicated by decision makers.

Facilitating continuous improvement within both the intelligence and risk analysis systems is difficult. Chris Bellavita cites Edwards Deming, an authority on continuous improvement, in his argument that the fear of new behavior, emergence, and imagination get in the way of system improvement and understanding the system processes that empower people to determine what needs to be done to facilitate continual improvement (Bellavita, 2005). Leadership charged with decision making must be invested in improving the intelligence and risk assessment systems. In doing so, they need to emphasize the importance of adaptation and the continuous refinement of intelligence and risk analysis in order to support their intelligence needs.

The common threads between intelligence and risk analysis do not end with information needs, analysis, mission similarities, and bias or external influences. The next section moves the discussion from general similarities to a comparison of the steps within the intelligence cycle with those in the risk management cycle.

C. COMPARISON OF THE INTELLIGENCE AND RISK MANAGEMENT CYCLES

It should not be surprising that the intelligence and risk management cycles share common attributes given their common goals of supporting policy and decision making with the analysis of pertinent data. Even though intelligence and risk management remain distinctly separate disciplines, they both rely on a cycle focused on the analysis of information. Increased understanding of risk analysis and management practices by intelligence professionals could provide insights to improve intelligence, and a greater knowledge of intelligence processes could assist risk management professionals to strengthen risk analysis and management practices. Both the intelligence cycle and the DHS risk management cycle are provided in Figure 6 to orient you to this comparison.

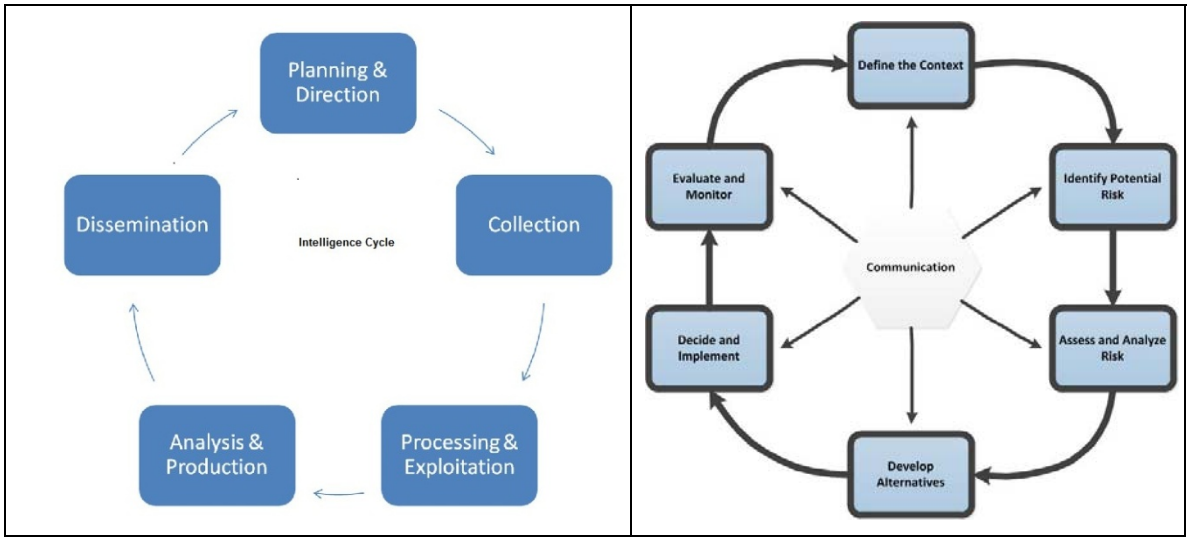

Figure 6. Comparison of the Intelligence Cycle from (Lowenthal, 2009 p. 65) and the DHS Risk Management Process (United States Department of Homeland Security (DHS), 2011 p. 15)

The first phase in both the intelligence cycle and the risk management process begins with the establishment of the scope. The intelligence cycle defines this initial step as *Planning and Direction*. In this step, the policy areas where intelligence can contribute are identified and prioritized (Lowenthal, 2009). Within the homeland security risk management process, the first phase is *Defining the Context.* This step defines the

requirements, constraints, and priorities for the decision or policy objectives to be supported by risk management (United States Department of Homeland Security (DHS), 2011). Additionally, the risk management process includes a step to *Identify Potential Risk* in this incipient phase. This step expands on defining the context by cataloging and categorizing the various risks to be considered (United States Department of Homeland Security (DHS), 2011). The first two steps in the Carnegie Mellon Risk-Ranking Method, provided in Figure 7, align with the scoping that occurs in the planning and direction step in the intelligence cycle, and the step to define the context in the DHS risk management model. The Carnegie Mellon Risk-Ranking Method provides the basis for comparative risk assessment described by Florig et al. (H. K. Florig et al., 2001). & Morgan et al. (Morgan, Florig, deKay, & Fischbeck, 2000).

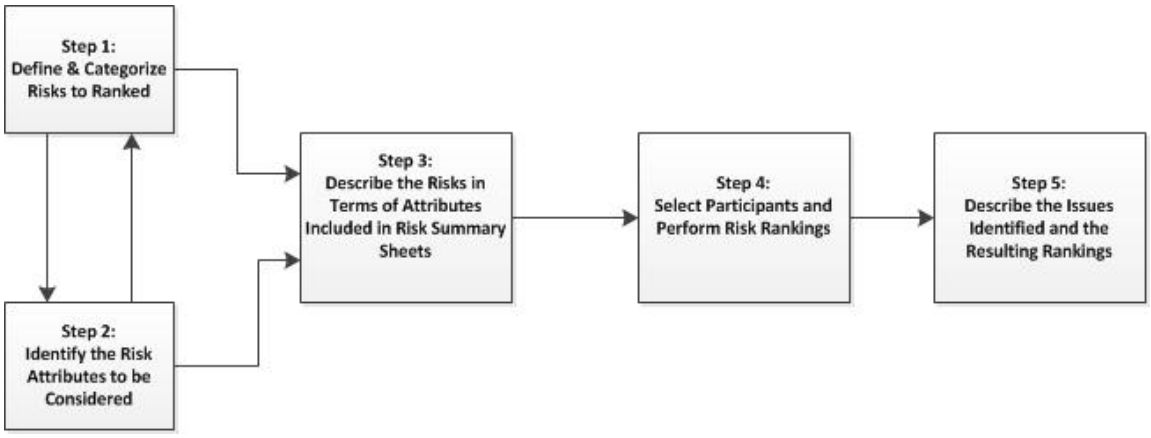

Figure 7. Carnegie Mellon Risk Ranking Method from (Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B., Fischbeck, P. S.,& DeKay, M. L., 2001)

The next phases in both the intelligence cycle and the risk management process include a major focus on gathering data. It is noteworthy that while activities associated with these phases are similar, there is a significant difference in how the activities are organized and broken down by each respective process. The intelligence cycle includes two separate steps that focus on gathering information and preparing it for analysis (Lowenthal, 2009 pp. 60–61). These steps are *Collection,* and *Processing and Exploitation.* Since data achieved though collection is often not ready for use by analysts,

the processing and exploitation of the data allows it to be translated and decoded from signals to images and intercepts that can be used by analysts (Lowenthal, 2009 p. 61). The next step in the homeland security risk management cycle is *Assess and Analyze Risk*. This involves selecting an appropriate risk assessment methodology, gathering required data, assess risk, validation of data inputs and outputs, and analyzing the results of the assessment (United States Department of Homeland Security (DHS), 2011 pp. 19–20). It should be noted that even though the risk management phase of assessing and analyzing risk does not include a step for processing and exploitation, this aspect should not be overlooked. Depending on which methodology and model are selected for risk analysis, geospatial and signals data may need to be processed and exploited before being incorporated into a model. Some examples where this is appropriate may include data from seismographs, flood gauges, or topographical data obtained with Light Detecting and Ranging (LIDAR) technology.

Analysis occurs in both the intelligence cycle and risk management cycle following the collection, processing, and exploitation of data. The intelligence cycle labels this step as *Analysis and Production*. In this phase, intelligence is analyzed and various products are produced to meet the needs established by the decision makers requiring intelligence support. This includes a range of products tailored to meet the near-term or long-range intelligence needs of policy and decision makers (Lowenthal, 2009). Although analysis begins with the step to assess and analyze risk in the homeland security risk management process, it continues into the step labeled as *Developing Alternatives*. The development of alternatives involves identifying a variety of risk management options that support the decision makers and policy objectives, and assessing the merits of each (United States Department of Homeland Security (DHS), 2011). The methodologies may differ between the intelligence process and that of risk management, but the common goal is to produce analytical products that meet the defined needs of policy and decision makers.

The differences between the intelligence cycle and the risk management cycle related to the collection, processing, exploitation and analysis of information extend well beyond the surface depicted in the process diagrams. These differences extend to the

culture and organizational mechanics of completing these various tasks. The U.S. intelligence recognizes that those performing analysis should drive data collection, however, in practice, this is rarely achieved because analysts rarely receive an explicit list of priorities from policy makers (Lowenthal, 2009). Analysts tend to be very involved with information collection within the risk management community (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). The collection, processing, and analysis disciplines within the intelligence community are distinctly separate disciplines, and the analysts are often marginalized with respect to influencing the data collection priorities needed to support analytical products (Lowenthal, 2009). The direct involvement of risk analysts in determining which data collection efforts are worth pursuing based on their ability to reduce uncertainty (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010 pp. 61).

The names and descriptions of the final phases of the intelligence and the risk management cycles are different; however, they accomplish very similar functions. The final phase of the intelligence cycle is *Dissemination*. In this step, the intelligence products are distributed to the decision makers and policy staff requiring the intelligence (Lowenthal, 2009). The risk management process implies dissemination while it labels the next step as *Deciding on and Implementation of Risk Management Strategies*. This involves providing the assessment of risk management options to the appropriate decision makers (United States Department of Homeland Security (DHS), 2011). The DHS risk management process follows with a feedback step, which is implied in the intelligence cycle. The common goals of these steps involve getting the processed information to those who need it to make decisions and receiving feedback on the products and additional needs.

D. INTELLIGENCE SUPPORT OF RISK ANALYSIS

Intelligence assessments play a significant role in risk analysis within the homeland security domain. Evidence for the importance of intelligence assessments in supporting risk analysis can be found by examining the various terrorism and

infrastructure risk assessment models, guidance and operational concepts for state and urban area fusion centers, and strategies for intelligence and homeland security.

The concept of risk analysis is focused on assigning probabilities to potential hazards or threats and gauging the subsequent impacts associated with the event. It is not considered a process for predicting the occurrence of a hazard and its impacts. The concept of probability is rooted in the mathematical and statistical communication of likelihood, and prediction implies a precise forecast about a hazard or threat and its consequences at some future point in time (Ropeik, 2010). The term prediction provides a false sense of accuracy that can undermine the confidence of decision makers in the risk assessments they use to manage homeland security risk (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). People generally hold preconceived notions of how mathematical and statistical patterns are supposed to work out; this framing effect, coupled with the innumeracy within the general population, contribute to the false sense of accuracy perceived with representations of probability (Ropeik, 2010).

Accuracy and consistency are important characteristics regarding intelligence estimates used for risk analysis. Estimates are not predictions but should be considered judgments that provide an educated perspective on the likely course of future events (Lowenthal, 2009 p. 136). Predictions imply a high degree of accuracy, which presents problems with the speculative nature of intelligence products. While intelligence analysts strive to be exceptional through accuracy, no one can be correct all of the time; hence, consistency is a better way to gauge the value of intelligence (Lowenthal, 2009 p. 148). Thus, striving for consistent intelligence assessments is more beneficial to risk analysts than trying to achieve completely accurate assessments. These subtle distinctions remain important considerations for incorporating intelligence products into risk analysis and management.

It is important to remember that uncertainty exists within the risk analysis products for both natural hazards and terrorist threats. However, expert judgments on the likelihood and consequences of terrorist threats are perceived to be less precise than those for natural hazards for two key reasons. First, human nature and intent is more difficult to

understand, predict, and model than the physical aspects of natural hazards. Secondly, more empirical data exists for natural hazards for experts to use in making risk assessments, where very little useful empirical data exists for experts to call upon in developing terrorism threat assessments (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010).

Risk analysis includes the common variables of threat, vulnerability, and consequence for virtually all homeland security risk assessment models, but the scope and content of intelligence products used for risk assessments vary widely. The intelligence assessments needed to support risk analysis differ significantly based on the detailed aspect of a specific threat to be analyzed (Baker et al., 2009). Furthermore, numeric values assigned to threat, vulnerability, and consequence are problematic for several reasons as pointed out by Tony Cox in his article, "*Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks*. First, he explains how threat estimates may be thwarted by attackers using intelligence about the threat assessment itself to determine when and where an attack is most likely to achieve its objectives. He also describes how vulnerability values are subject to adapt plans in order to continue with attacks when obstacles are identified. These types of variable factors are hard to quantify and rely on expert opinion from the intelligence community in order to produce assessment of terrorism threats for risk analysis and management (Cox Jr., L. A. (Tony), 2008).

A report from the Homeland Security Institute identifies five main types of intelligence threat judgments that support terrorism risk assessment. These include: estimation on the likelihood of attacks, attack method, type of adversary making the attack, and the adaptability and ability of the attacker to acquire countermeasures (Baker et al., 2009, p. 22). Each of these expert conclusions also depend on any number of specific issues that frame the assessment based on the needs of the decision maker or intelligence consumer. Intelligence estimates on the likelihood and frequency of attacks depend largely on timeframes to delineate the bounds of judgment. Attack assessments depend on target and weapon types, domain, tactics and methodology, and terrorist characteristics, such as ideology, group identity or lone wolf, and whether or not the

attacker is foreign or domestic (Baker et al., 2009). These threat judgments can be individually or collaboratively produced by any number of sources at all levels of government and the private sector.

The Homeland Security Institute report identifies several challenges for producing threat judgments in support of homeland security risk assessments. These challenges impede collaboration and can largely be attributed to the distinct cultural differences between the intelligence and risk analysis disciplines. Risk analysis generally includes multiple component inputs into a highly structured model. Threat assessments represent one input into the process. The production of intelligence threat assessments represents a more fluid process driven by the dynamic and conditional nature of threats applied to scenario planning (Cummings, McGarvey, & Vinch, 2006b). Additionally, the discipline of risk analysis relies strongly on empirical models driven by quantifiable probabilistic, vulnerability, and consequence inputs. In contrast, intelligence assessments provide a more qualitative analysis that includes substantial uncertainty. This allows the intelligence assessments to account for the variables associated with adaptive adversaries and tactics in a perpetually changing environment. The periodic interaction with the intelligence analysts common to most risk analysis processes can exacerbate these challenges. Problems associated with limited interaction include inadequate preparation, differing points of view and understanding about scenarios, and the lack of transparency and follow-up can hamper productive collaboration between intelligence and risk analysts (Baker et al., 2009).

The afore-mentioned report also describes three primary approaches to collaboration between the intelligence and risk analysis communities within the homeland security context. These approaches are categorized by frequency of interaction to include continuous, periodic, and no direct interaction (Baker et al., 2009). The continuous interaction approach includes cross-disciplinary staffing and affords a high degree of collaboration. Naturally, this improves communication between intelligence and risk analysts and provides the foundation for a more effective relationship. However, the high investment of resources and personnel make this approach difficult to implement, especially within the construct of state and local government.

Periodic interaction between intelligence analysts and their risk counterparts requires significant preparation activities by both parties to maximize the effectiveness of limited meeting time. While this approach limits the investment of staff and resources and provides greater flexibility by affording the opportunity to take advantage of a larger pool of intelligence experts, several limitations should be considered. These include the need for intelligence analysts to make time to elicit threat analyses requirements, and the need for risk analysts to be much more familiar with the intelligence community, so they can direct their intelligence needs to the appropriate technical experts (Baker et al., 2009). This intermittent interaction can foster issues known to impede collaborative work to include divergent goals, focusing on internal agency concerns and priorities in lieu of those held by the collective group, absence of clear goals, want of accountability, lack of familiarity with other organizations and insufficient communication and information sharing (Hocevar, S. ,P., Thomas, G. F., & Jansen, E., 2006).

The third approach where no direct interaction occurs reduces workloads, conserves resources, and avoids coordination issues (Baker et al., 2009). However, it also reduces the degree to which the knowledge and expertise of the intelligence community is leveraged to improve risk analysis. This limited approach strengthens the effect of barrier factors referenced in the previous paragraph on collaborative activity.(Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006) The absence of direct interaction also may lead risk analysts to draw the wrong conclusions and make invalid inferences from intelligence products that were not tailored to their specific needs. This segregation between intelligence analysts and the risk analysts is similar to the disconnect between the intelligence collection discipline and the intelligence analysts, as described previously. Mark Lowenthal articulates this challenge in his description of the disconnect between collection and analysis with these words, “It is difficult to task a system that one does not fully understand” (Lowenthal, 2009).

The various contributions of intelligence assessments to the wide array of risk analysis tools and methodologies become apparent upon a cursory examination of their design and function. The various risk analysis techniques, tools and models are each designed for a specific purpose and to assist risk management at all levels (Cummings,

McGarvey, & Vinch, 2006b). These include the tactical focus of mission-based risk assessment, the operational focus of system based risk management, and the strategic focus of risk-informed decision making (Cummings, McGarvey, & Vinch, 2006a). Additionally, the level of collaboration between the intelligence community and the risk analysts differs substantially based on the risk analysis model and context (Baker et al., 2009).

The Strategic Homeland Infrastructure Risk Assessment (SHIRA) provides a general snapshot of risk from natural hazards and terrorism to the critical infrastructure in the nation. This strategic view of risk incorporates intelligence into risk analysis using a mixed staffing approach. This occurs at the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). The continuous interaction between intelligence and risk analysts at the HITRAC supports strategic level risk analysis across all sectors (Baker et al., 2009). The Coast Guard's Maritime Security Risk Analysis Model (MSRAM) provides another example of continuous interaction between the intelligence and risk analysis communities. However, it does not just rely on traditional classified intelligence sources; instead it integrates locally available unclassified information. This enhances the site specific effectiveness of the product and makes the assessment easier to share among state and local partners (Baker et al., 2009). In contrast, a strategic risk assessment approach that aggregates expert opinions and ranks threats at a strategic level, such as the Analytic Hierarchy Process (AHP), may only require periodic interaction (Cummings, McGarvey, & Vinch, 2006b).While the limited interaction can impede collaboration, the AHP-based approach produces a comparative risk ranking similar to the Carnegie Mellon Risk Ranking Method used in comparative risk assessment. This process defines and categorizes risks and attributes to form a basis of comparison (Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B., Fischbeck, P. S., & DeKay, M. L., 2001).

The Risk Management Analysis Process (RMAP) employed by the Transportation Security Administration (TSA) provides an operational risk management example of how periodic interaction between the intelligence and risk analysis communities serves to manage risks to commercial aviation security. This process incorporates information ranging from Protected Critical Infrastructure Information (PCII), Sensitive Security

Information (SSI), (Cummings, McGarvey, & Vinch, 2006b) For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and private sector proprietary information. This process provides a good example of how different types of information can be leveraged among a diverse group of analysts to generate a collaborative intelligence driven risk analysis. This requires intelligence analysts to think in unfamiliar ways, and work with nontraditional partners. While periodic interaction could be seen as a handicap to this process, it motivates risk analysts to make decisions that use analytical resources from the intelligence community wisely (Baker et al., 2009).

E. BENEFITS OF ENHANCED COLLABORATION AMONG INTELLIGENCE AND RISK ANALYSIS

Multiple sources support the notion that greater collaboration needs to occur between the intelligence and risk analysis communities. The Government Accountability Office (GAO) convened a forum of risk management experts in 2008. Participants in the forum identified the need for risk analysis training for intelligence analysts (Government Accountability Office (GAO), 2008). Greater collaboration and integration of intelligence and risk analysis to support risk management is the focus of a report published by the Homeland Security Institute in 2009 (Baker et al., 2009). Additionally, a recent article titled *Intelligence-led Mitigation* also emphasized the importance of the relationship between the intelligence and risk management process (Townsend, Sullivan, Monahan, & Donnelly, 2010).

A report from the Homeland Security Institute published in 2009 provides four key findings related to collaboration between the intelligence community and the risk analysis community. These findings call for greater cross-discipline familiarity, advancing beyond a "Supply and Demand" perspective to a fully symbiotic relationship, systematic engagement to achieve better threat judgments, the need for additional research on how to improve threat judgments required for homeland security risk assessments (Baker et al., 2009). These findings provide a conceptual framework to explore collaboration between the intelligence and risk analysis communities.

The U.S. Intelligence Community recognizes the need for improving collaboration among the traditional members of the intelligence community and with nontraditional players such as state and local governments. Evidence of this can be found in the National Intelligence Strategy, which clearly articulates a strategic need to improve collaboration and build partnerships (The Office of the Director of National Intelligence, 2009). Former Director of National Intelligence Mike McConnell makes a compelling argument that the intelligence community needs to develop a shared approach that will promote effective coordination and integration of work thus increasing the agility of agencies to cope with the dynamic landscape of security threats. He identifies the importance of integrating law enforcement into the intelligence community and the success that DHS and the FBI have achieved in achieving an integrated approach (McConnell, 2007). McConnell asserts that the intelligence community needs to abandon the long-standing policy of providing information on a "need-to-know" basis and replace it with a cultural standard of "responsibility to provide" while providing reasonable and prudent protections (McConnell, 2007). This is a central concept for improving collaboration among the intelligence community and extending it to the risk analysis community (McConnell, 2007).

Several examples of organizational collaboration between intelligence and risk analysis functions exist. The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) demonstrates a collaborative relationship that combines intelligence with risk information to produce assessments of risk for all hazards and threats to infrastructure networks of national significance. Effective information sharing among local, state, and federal government and the private sector allow the HITRAC to produce quality risk and threat assessments that are made available to appropriate stakeholder groups (U.S Department of Homeland Security, February 2011). The Interagency Threat Assessment and Coordination Group (ITACG) provides another example of collaborative work between the intelligence and risk analysis community. Although the ITACG does not have a risk analysis function, it does support risk analysis within DHS organizational components, state, and local government. It seeks to address the intelligence needs of state and local government by including state and local personnel on the ITACG staff

detail (*Department of homeland security interaction with state and local fusion centers concept of operations* 2008). State and local fusion centers also provide another example of collaboration between intelligence and risk analysis.

The risk analysis process can inform the intelligence process to produce more refined threat assessments. This comports with the notion that greater collaboration is needed between the risk analysis community and the intelligence community, and that analysts need to be more involved with shaping the scope of threat assessments. In a working paper for the Rand Corporation, Henry Willis suggests that the products of risk analysis can improve intelligence products, and that risk analysis can assist in shaping intelligence collection priorities (Willis, 2007).

Terrorism threat assessments provide an example of how risk and vulnerability analysis can help improve intelligence assessments. Terrorism threat analysis depends on opportunity, intent to act (including goals and objectives of terrorist), and the capacity to carry out the attack. Willis argues that terrorism risk analysis provides a structure to incorporate intelligence about the goals, objectives, and capabilities of terrorist groups with the vulnerabilities from various attack modes, and consequences of different types of attacks on different targets to focus on scenarios that represent the greatest risk (Willis, 2007). The ability to focus on the scenarios that provide the greatest risk is precisely the type of information required by principal decision makers in developing homeland security risk management strategies, although intelligence limitations may limit the usefulness of this type of analysis to strategic or operational risk management activities. The results of the risk analysis can be incorporated back into the intelligence process at the analysis and production stage. This corresponds with the idea of the iterative scenario analysis process that incorporates the findings and observations associated with previous scenarios to shape the evolution of the next scenario in the sequence for planning purposes (Van der Heijden, 2005). The results of this iterative scenario planning process can be used in red teaming to dissect various attack scenarios and vulnerabilities to drive additional collection activities and select appropriate countermeasure strategies (Willis, 2007). The benefits to both the intelligence community and risk analysis community are best summarized in this statement from the *Risk Analysis and Intelligence Communities*

Final Report from the Homeland Security Institute, "The stakes for both communities in improving collaboration mainly hinge on enhancing each community's organizational performance" (Baker et al., 2009).

While the mutual benefits of collaboration between the intelligence community and the risk analysis community are clear, several challenges must be accounted for and effectively managed in order to avoid undermining both the intelligence and risk analysis processes. Mr. Willis identifies four key challenges in his working paper: basing analyses on available information, matching the resolution of analysis to assessment problem, applying the best practices from risk analysis to create intelligence assessments, and avoiding blinding analysts to surprise (Willis, 2007). Generally, risk analysis models emphasize deliberative quantitative approaches that are transparent and easy to replicate so that risk can be communicated effectively. This represents a substantial difference from terrorism threat assessments that are more qualitative in nature to address the inherent uncertainty associated with terrorism risk (Cox Jr., Louis A. (Tony), 2008).

Limitations of available data pose a significant challenge to the fusion of the intelligence and risk analysis processes. Risk analysis draws upon years of expertise that provide a strong methodical foundation for experts and sophisticated models that require specific data inputs (Government Accountability Office (GAO), 2008). Without these inputs, the analysis goes nowhere and effort is wasted. Intelligence assessments related to terrorism do not have years of experience, empirical data, and sophisticated models to draw upon. The data and assumptions that produce a risk assessment also define its limitations, and thus, risk assessments are blind to scenarios or assumptions that are not included in the analysis (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). This also relates to the central idea that the framing of data and assumptions is part of human nature as Ropeik argues in his book, "*How Risky Is It, Really?"* (Ropeik, 2010). The best contextual example of this issue can be found in the intelligence failure and lack of institutional imagination expressed in the 9/11 Commission Report (Kean & Hamilton, L. H., 2004).

Risk management takes place at different decision-making levels each with different intelligence support requirements. Risk assessments support risk management at tactical, operational, and strategic decision levels, and each requires a different level of resolution to support decision making (Cummings, McGarvey, & Vinch, 2006a). Too much or too little detail in assessments can confuse issues and incorrectly frame risk issues at each level of decision making.

F. INTELLIGENCE-LED RISK MANAGEMENT

State and local governments represent the level of government most often directly impacted by the consequences of the wide range of homeland security threats and hazards, and thus, have a large stake in developing and implementing sound risk management strategies. This fact is recognized by the collaborative white paper, "*Recommendations for an Effective National Mitigation Effort"* (National Emergency Management Association, 2009). This premise is also supported by the Disaster Mitigation Act of 2000, which promotes a national strategy to manage natural disaster risks through state and local hazard mitigation plans (Federal Emergency Management Agency (FEMA), 2007). Additionally, both the National Strategy for Homeland Security and the National Infrastructure Protection Plan recognize that the majority of the homeland security risks exist within the private sector and in the jurisdiction of a unit of state or local government.

The concept of "Intelligence-Led Mitigation" provides a framework that applies the intelligence concepts intrinsic to community policing in a broader construct to address the intelligence needs of multiple public safety disciplines. "*Intelligence-Led Mitigation*" is described as, "management philosophy and business process to proactively guide strategic, operational, and tactical decisions for mitigating the effects of intentional, accidental, and natural incidents," and they offer this concept as a vehicle to address the existing gaps in the intelligence products available to support resource decisions (Townsend et al., 2010). The Police Executive Research Forum makes the point that intelligence is a decision-making tool, and the need to support decision making extends beyond artificial boundaries created by missions, jurisdictions, and discipline (Police Executive Research Forum, 2005). This point is echoed by the authors of *Intelligence-*

Led Mitigation (Townsend et al., 2010). Two key principles provide the basis for intelligence-led mitigation: first, intelligence products are needed to support the decision-making process for allocating resources for mitigation; and second, that decision makers need to clearly communicate their intelligence/information needs (Townsend et al., 2010). Ultimately, the concept of Intelligence-led mitigation suggests that the application of the intelligence process provides an added value to the decision-making process for mitigating any hazard, not just criminal and terrorism threats.

Intelligence-led risk management represents the fusion of the intelligence cycle and risk management process. This concept builds on the key elements offered by *Intelligence-led Mitigation* by injecting the principles of intelligence cycle into the development of the risk management culture within the homeland security enterprise. Figure 8 depicts how the intelligence cycle and risk management process are fused to promote risk management driven by intelligence. The hub of the intelligence-led risk management process is communication. A shared understanding of the risk and its associated factors is achieved through consistent communications with those charged with decision making, managing aspects of the cycle, and analyzing and producing assessments throughout the process.

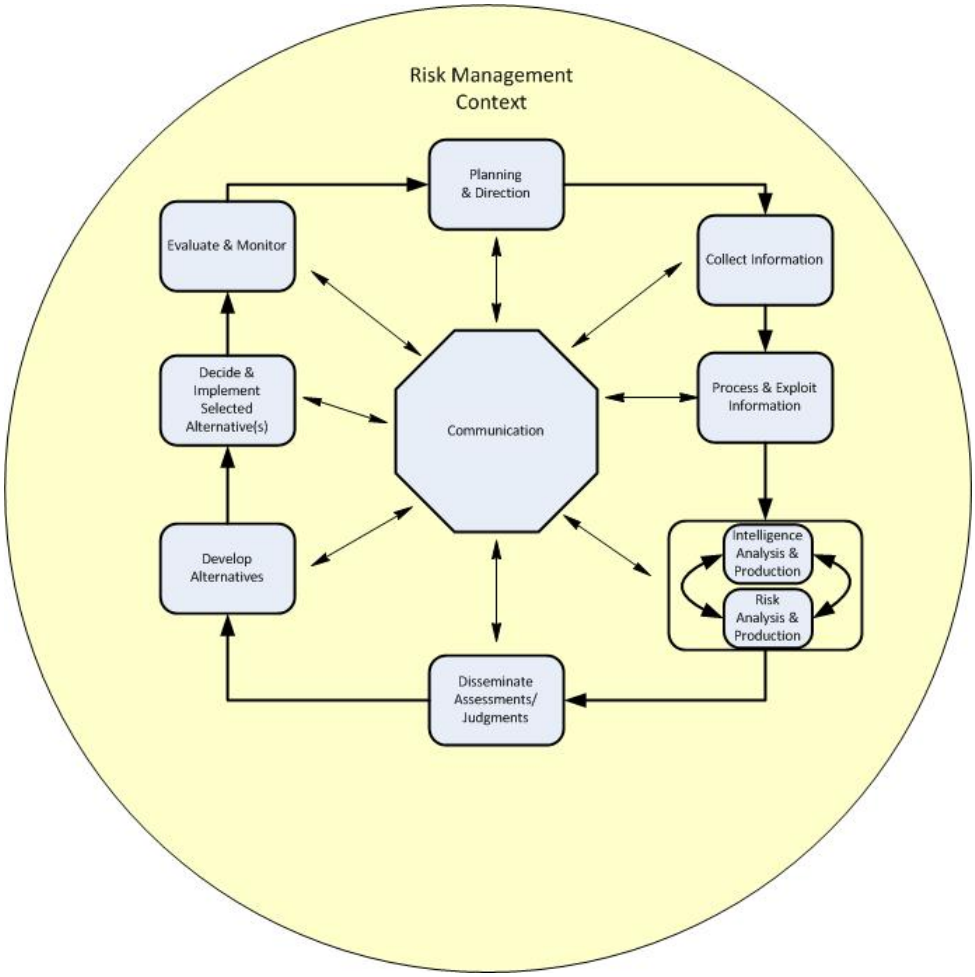

Figure 8 Intelligence-Led Risk Management

The Intelligence-Led Risk Management process takes place within the context established by leadership, and those ultimately responsible for making risk management decisions. Several factors need consideration to frame the risk management context, which include: goals and objectives, mission space and organizational values, policies, decision scope and criticality, decision makers and stakeholders, decision timeframe, capabilities and resources, risk tolerance, and information availability (United States Department of Homeland Security (DHS), 2011). The context provides the boundaries for the risk management efforts. The information relevant to these factors must be shared with those involved in directing the collection, processing, exploitation and analysis for quality results and efficiency. Providing this information helps analyst direct collection and communicates priorities for processing and exploitation thus allowing their products

to provide the required support of the decision process. This fits with the notion of analyst driven collection, offered by Lowenthal, that the U.S. intelligence strives for, but ultimately finds elusive (Lowenthal, 2009).

The Intelligence-Led Risk Management process is a cycle that begins with developing a plan and directing the efforts of process components. This first step includes planning and directing the collection of information, analysis, assessment/judgment products to be developed, and how they will be disseminated. The intelligence analysis/production step and risk analysis/production step represent a codependent relationship within the cycle. These two interdependent steps occur in parallel providing information to each other that continue to refine both intelligence and risk assessments.

Intelligence-Led Risk Management cycle continues with dissemination of the assessment products after they have been refined to the appropriate resolution. When the assessments are received by the appropriate parties, a spectrum of alternatives to address the risk is generated for the decision makers. Upon the presentation of the alternatives, the decision makers select the alternatives to be implemented. After, the implementation, the risk is monitored and reevaluated. Hence the cycle perpetuates.

State and Local Fusion Centers (SLFCs) provide a capable and logical mechanism to implement the idea of Intelligence-Led Risk Management, thus improving coordination and collaboration between intelligence and risk analysis activities at the state and local level of government. DHS guidance on fusion center capabilities stresses the importance of data collection and analysis to meet the strategic mission of the center defined by the state or urban area which it serves (United States. Department of Homeland Security, 2008).

State and local governments need an intelligence driven approach for risk management. Dr. James Steiner provides a reasonable argument that intelligence needs of state governments extend beyond the tactical or operational intelligence needed to support law enforcement and include the need to provide strategic intelligence, as well, in order to effectively manage the unique threats and risks to any given state (Steiner, 2009). Governors and local government elected officials need strategic level decision-making

support to adequately address and manage the various risks and threats present in an interconnected world (Chen, 2009). The U.S. Department of Homeland Security identifies risk assessment as a baseline capability for SLFCs (United States. Department of Homeland Security, 2008). DHS also identifies a mission similar to the mission of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) for state and local fusion centers. This mission is to ensure the inclusion of critical infrastructure and key resource information in state and regional risk assessments (*Critical infrastructure and key resources (CIKR): Protection capabilities for fusion centers [December 2008] [an appendix to the 'baseline capabilities for state and major urban area fusion centers']*, 2008).

In fact, a majority of state and local fusion centers examined for a 2007 report to Congress indicated that they saw their primary mission as one of prevention and mitigation (Masse, T., Rollins, J., 2007). The location of fusion centers within state and local government afford them the opportunity to support emergency services and homeland security operations with accurate and timely intelligence. While DHS supports the creation and operation of SLFCs, they are developed and maintained by the respective state and local governments they serve. Fusion centers may strive to achieve the capabilities specified by DHS, their scope, capabilities, and structures are determined by the unique needs and resources available to the jurisdictions that created them.

State and Local Fusion Centers (SLFCs) provide a structure that can incorporate some of the best attributes from the Transportation Security Administration's Risk Management Analysis Process (RMAP) and the U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) into state and local risk assessments. The RMAP process compiles a variety of information with different handling requirement from multiple sources to include the private sector (Baker et al., 2009). The flexibility inherent to SLFCs allows them to organize their operations in such a manner to handle different types of information from multiple sources. This flexibility also provides an opportunity for intelligence analysts and risk analysts to work closely together on a regular basis, which improves the ability of both intelligence and risk analysts to understand and appreciate the thought processes of the other. An important factor of the MSRAM

success is the continuous interaction between intelligence analysts at the national level and state and local stakeholders. This interaction provides a methodology to incorporate locally available unclassified information into the process without the classification barriers common to traditional intelligence sources (Baker et al., 2009). The end result is a higher quality risk assessment that is more easily shared with state and local stakeholders.

The specific intelligence and risk analysis needs of local, state, and federal government differ significantly in terms of their scope. Their utility depends on active participation and possession of the collection and analysis of information, and transparency. Willis articulates the importance of this point in his working paper (Willis, 2007). A report to Congress also emphasizes the importance of state and local ownership in the fusion centers they sponsor and operate (Masse, T., Rollins, J., 2007). Additionally, Dr. Steiner emphasizes the need for state and local intelligence enterprises to know their mission, and most importantly their primary intelligence customers (Steiner, 2009).

The concept of intelligence-led risk management paired with state and local fusion centers provides a viable set of tools to integrate intelligence and risk management within state and local government to drive the risk management process. Although nearly forty percent of fusion centers consider themselves to be all-crimes/all-hazards in nature, the term “all-hazards” is not consistently used throughout the SLFC community (Masse, T., Rollins, J., 2007). This issue in itself is not problematic as long as the agencies participating and relying on the respective state and local fusion centers for intelligence and analysis have a common understanding of how the term all-hazards is applied within their construct.

As the idea of Intelligence-Led Risk Management suggests, the strengths of both intelligence and risk analysis can be leveraged to support insightful risk management decision making throughout the homeland security enterprise. The fusion of these independent, but complementary disciplines, can support strategic, operational, and tactical decisions for managing risks prior to, during, and in the aftermath of any kind of incident with homeland security implications. The greatest beneficiaries will likely be local and state governments who bear the greatest share of responsibility for domestic of

risk management in our federal system of government. This approach will rely on effective collaboration to overcome the cultural barriers and complex problems inherent to the homeland security enterprise.

G. CONCLUSION

A close relationship exists between the concepts of intelligence and risk management. While both risk management and intelligence remain important independent disciplines within the context of homeland security, shared learning and exchange between them can be mutually beneficial. Risk analysis provides the key link between the intelligence and risk management.

Intelligence-Led Risk Management provides one approach to draw the intelligence and risk management disciplines together. By fusing the intelligence and risk management cycles, Intelligence-Led Risk Management can support the information needs of decision makers for risk management. This concept enables decision makers to prioritize and direct the collection and analysis of information to support the goals and objectives within risk management context.

Collaboration and strategic planning play an important role in linking the intelligence and risk management functions within homeland security. The next chapter explores collaboration and strategic planning with a focus on how to improve the linkage between intelligence and risk management.

IV. COLLABORATION AND PLANNING FOR STRATEGIC RISK MANAGEMENT

The concept of collaboration permeates the homeland security enterprise by design and necessity. Even the casual observer can identify risk management and intelligence as inherent pieces of the homeland security enterprise requiring collaboration, but the breadth and complexity of these issues continue to pose strategic and operational challenges to collaborative efforts among all homeland security stakeholders. The scope of risk management permeates the homeland security enterprise requiring collaborative work to support many applications to include; strategic planning, capabilities-based, planning, resource decisions, operational planning, exercise planning, real-world event response and recovery, and research and development, as described in the Homeland Security Risk Management Doctrine published in April 2011.

The concept of Intelligence-Led Risk Management provides a vehicle to promote collaboration between intelligence and risk management in support of informed decision making within the homeland security enterprise. As such, the implementation of Intelligence-Led Risk Management needs to capitalize on those factors that enable and promote collaboration while effectively managing the issues that inhibit effective collaboration. This chapter explores both the enabling and factors and impediments. It also seeks to explain their influence on the success or failure of collaborative efforts. These factors relate to the institutional risks that are associated with an organizations ability to build and maintain effective management and control systems and adapt to dynamic organizational requirements.

This chapter identifies factors that influence collaboration, and seeks to develop strategies to foster and encourage collaboration among decision makers and stakeholders from all levels of government, the private sector, and among the many disciplines involved in managing risks within the homeland security environment. These factors will be applied to strategic thought and planning principles and the Cynefin Framework. This

fusion of concepts will produce guiding principles that ultimately enable Intelligence-Led Risk Management to promote collaboration and strategic adaptability within the homeland security risk management landscape.

A. THE NEED FOR COLLABORATION IN RISK MANAGEMENT

Risk management and intelligence within the homeland security context share a codependent relationship, as described in previous chapters. In this sense, risk management relies on threat assessments from the intelligence community to assess risk; and the intelligence community requires direction and an understanding of expectation placed on the assessment from the risk analysts.

The need for greater collaboration in homeland security risk management has been identified in several recent documents and studies. The recently published Homeland Security Presidential Policy Directive-8, for example, emphasizes a collaborative preparedness framework. Risk management and intelligence and information sharing are also both listed as common target capabilities in the DHS Target Capabilities list, which implies a broad scope with an inherent need for collaborative work (United States. Department of Homeland Security, 2007). The National Emergency Management Association identified these three strategic themes in building a national mitigation effort to manage risks, all of which either directly assert or imply the need for collaboration: broader collaborative partnerships, total-hazard awareness, and full spectrum community-to-federal emphasis (National Emergency Management Association, 2009). Additionally, the 2009 report from the Homeland Security Institute identifies specific needs for improving collaboration between the risk analysis intelligence communities, which include; improving cross-discipline familiarity, moving beyond a supply and demand to a mutually beneficial relationship, and leveraging systematic engagement to achieve better threat judgments (Baker et al., 2009). These examples are not outliers and comport with the recommendations and findings of additional reports and strategies within the homeland security domain that call for stronger collaborative efforts.

With the emphasis and importance placed on collaboration within the homeland security environment, we need to consider the question: why does collaboration continue to endure as a challenge for local, state, and federal government and the private sector? The homeland security enterprise continues to demonstrate shortfalls in its collaborative ability through poor information sharing among agencies, confusion over inter-organizational relationships, competing roles and responsibilities, and shortcoming in leadership (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). The notion that collaboration is an important component of the homeland security enterprise, and that we should do a better job of collaborating at each level of government and between disciplines, has been established and reiterated through numerous studies and reports. But as Hocevar, Jansen, and Thomas observe, studies addressing "how" to collaborate are far fewer that the ones that define the need to collaborate, and thus, we should develop a better understanding of how to collaborate if we are going to be successful (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011).

B. HOW TO COLLABORATE: ENABLERS & BARRIERS

To understand what enables or arrests collaborative efforts, we need to first understand the concept of collaboration within the homeland security context. Pelfrey defines collaboration as, "agencies, organizations, and individuals from many tiers of public and private sectors, working, training, and exercising together for the common purpose of preventing terrorist threats to people or property." (Pelfrey, 2005). While sound, this definition misses several key elements found in this definition offered by a public agency director: "*Collaboration is the act or process of "shared creation" or discovery. [It] involves the creation of new value by doing something new or different*;" (Thomson & Perry, 2006). Two key ideas missing from Pelfrey's definition are those of "shared creation" and "discovery." These ideas provide an added value to the collaborating organizations that allow them to redefine paradigms and adapt their practices accordingly. The notion of shared creation and discovery align with the idea of "shared learning," which is identified as a lateral mechanism for enabling collaboration (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). For our purposes, we will combine these concepts to define collaboration as, *agencies, organizations, and individuals from*

many tiers of public and private sectors working together to develop a common understanding of homeland security risks and threats and to create effective strategies to manage those risks through shared discovery.

Hocevar, Jansen and Thomas provide insight into the ability of organizations to collaborate, which they identify as Inter-organizational Collaborative Capacity (ICC), and define it as "the capability of organizations (or a set of organizations) to enter into, develop, and sustain inter-organizational systems in pursuit of collective outcomes." (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). As shown in Figure 9, their construct of collaborative capacity involves five key components, which include: purpose and strategy, structure, lateral mechanisms, incentives, and people (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). Thompson and Perry provide a different perspective in which they identify the five dimensions of collaboration that include; governance, administration, autonomy, mutuality, and trust and reciprocity (Thomson & Perry, 2006). These perspectives differ significantly and complement each other nicely in exploring how organizations can collaborate within the homeland security environment. The ICC model provides a vehicle to assess the various factors that enable an organization to collaborate with others (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). Thompson and Perry's offer a framework with five dimensions to assess the process of collaboration between organizations (Thomson & Perry, 2006).

The ICC Model builds on a study conducted by Hocevar, Jansen and Thomas that identifies two categories identified as "success" and "barrier" factors within the five domains of organizational design. Their analysis provides insight on how they influence organizational capacity to collaborate. Both categories are further stratified according to the organizational design components that include; purpose and strategy, structure, lateral mechanisms, incentives, and people (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006). Effective collaboration remains elusive without a number of conditions, which include a perception of need to collaborate, common goals, adaptability, interpersonal networks, the ability and willingness to share information, leadership, and mutual trust (Hocevar, S.

P., Jansen, E., & Thomas, G. F., 2011). Table 2 lists both the "success" and "barrier" factors for each of the organizational design aspects (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006 p. 8).

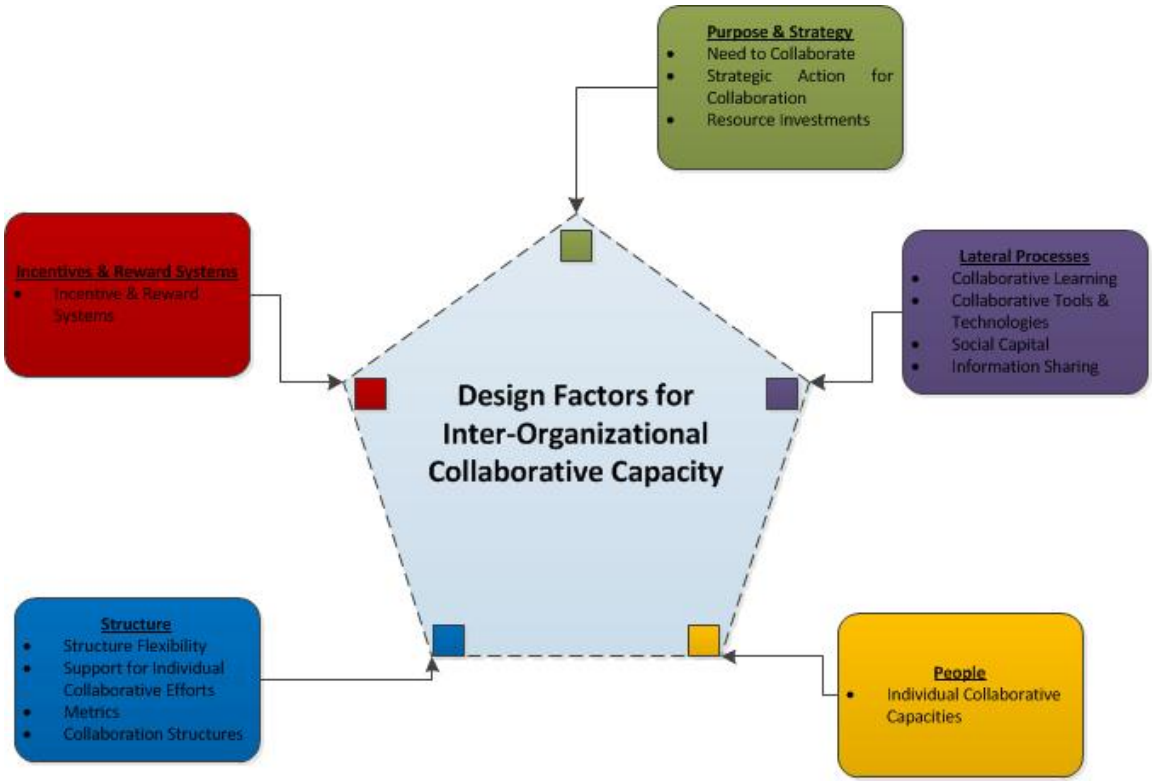

Figure 9. Inter-Organizational Collaborative Capacity Model from (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011)

Table 2. Factors Affecting Inter-Organizational Collaboration from (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006)

Factors Affecting Inter-Organizational Collaboration		
Organizational Design Component	**"Success" or Enabling Factors**	**"Barrier" or Inhibiting Factors**
Purpose & Strategy	• Feeling of "need" to collaborate • Common Goal • Recognized interdependence • Adaptable to interests of other organizations	• Divergent goals • Focus on single agency or organization • Lack of goal clarity • Not adaptable to interests of other organizations
Structure	• Formalized coordination roles • Sufficient authority of participants	• Impeding rules / policies • Inadequate authority of participants • Inadequate resources • Lack of accountability • Lack of formal roles / procedures for managing collaboration
Lateral Mechanisms	• Social capital • Effective communication & information exchange	• Lack of familiarity with other organizations • Inadequate communication and information sharing • Distrust
Incentives	• Leadership support and commitment • Collaboration requirement for funding • Acknowledged benefits • Absence of competitive rivalries	• Competition for resources • Territory • Organizational-level distrust • Lack of mutual respect • Apathy
People	• Appreciation of others' perspectives • Competency for collaboration • Trust • Commitment & motivation	• Lack of competency • Arrogance • Hostility • Animosity

The five domains and thirteen factors provided in the Inter-organizational Collaborative Capacity (ICC) model developed by Hocevar, Jansen and Thomas provide

a useful frame to examine interagency collaboration. The findings of several reports related to interagency collaboration in government fit nicely within the ICC framework (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). The five domains within the ICC model generally align well with four of the five dimensions of collaboration offered by Thompson and Perry. The fifth dimension offers a different perspective that offers insight into conflict within collaborative organizations.

The first two dimensions offered by Thompson and Perry include governance and administration, which are structural in nature and align with the structural domain and factors from the ICC model. Governance addresses the formal and informal structuring of how organizations jointly make decisions and reach agreement. The governance concept implies the absence of a hierarchical scheme to divide labor, an awareness that decisions need to be reached, an acceptance that collaborating entities have their own interests and that decisions represent consensus and not coalitions. Additionally, governance supports information sharing, transparency, and respect for diverging points of view (Thomson & Perry, 2006 p. 24). This point is echoed in the research conducted by Hocevar, Jansen and Thomas that indicates the need for a shared purpose, goals, and structured process to reach consensus, while avoiding an overly centralized top-down hierarchy(Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011). The administrative dimension provides the mechanism to move the governance to action. The lateral nature of collaborative groups still requires administrative oversight, which is accomplished by partners assuming different roles for which they are well suited. Aside from the leadership, technical and other administrative support roles, the management of relationships between organizations also plays an important role (Thomson & Perry, 2006 p. 25).

Thompson and Perry's next two dimensions, which include mutuality, trust and reciprocity, align with the lateral mechanisms, incentives, and people domains of the ICC model. The mutuality dimension represents symbiosis and interdependence within the collaborative structure (Thomson & Perry, 2006 p. 27). The ability of mutuality and lateral mechanisms to enable successful collaboration depends on establishing linkages that correspond to the interdependence of agencies and organizations (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006 p. 22). Thompson and Perry explain the concept of

trust and reciprocity in a context that manifests in two separate ways, which are short-term or contingent, and long-term or obligatory. The short-term/contingent variation of reciprocity dominates early collaborative efforts in which the willingness of collaborating partners to interact and share with others depends on the willingness of the other partners to do the same. They go on to explain that collaborative partnerships can evolve to long-term/obligatory reciprocity over time with continued interaction where trust and obligation motivate partners to engage in collaborative activity (Thomson & Perry, 2006 p. 27).

Thompson and Perry's final dimension of collaboration is autonomy. It does not align with the ICC model, but it does offer insight into how conflict can develop within collaborative structures. The concept of the autonomy dimension stems from the reality that members of collaborative groups actually have two separate identities; one for their organization and its authorities, and another one as a member of the collaborative group. This creates an internal struggle between organizational self-interest and the interests of the collective group (Thomson & Perry, 2006 p. 26). This reality emphasizes the importance of conflict management to address conflict within the coordination group and potential conflict with an individual organization. Thus, conflict management should be incorporated into the guidance and administrative components of the collaborative framework.

Weiss and Hughes offer some key ideas on how to manage and benefit from conflict in collaborative environments. They propose that structured and consistent approach for conflict resolution within the group coupled with establishing ordered criteria to evaluate trade-offs preserve integrity and collaborative relationships. Additionally, they emphasize the importance of joint and transparent escalation in those circumstances where resolution cannot be achieved at the point of conflict (Weiss, J., & Hughes, J., 2005). The ideas from Weiss and Hughes fit with the concept of structure from the ICC model, and the governance and administration dimensions from Thompson and Perry's model. Together these concepts support structure, consistency, and transparency with respect to conflict management.

The structure and administrative aspects of collaboration, described in the ICC model and by Thompson and Perry, can easily be seen in the homeland security context. State and major urban area fusion centers provide a visible example of these elements working together to enable collaboration that is relevant to intelligence and risk management. The ICC strategy domain is represented by the fact that fusion centers were born from a common need among agencies to enhance what was communicated in the Interim National Preparedness Goal (*Interim National Preparedness Goal: Homeland Security Presidential Directive 8: National Preparedness,* 2005). The ICC structure domain and Thompson and Perry's structure and administration dimensions are recognized in the governance, concept of operations, and procedures as recommended by the baseline capabilities produced by DHS (United States. Department of Homeland Security, 2008).

Lateral mechanisms, described in the ICC model, can also be seen in the homeland security fusion centers. The mechanisms for information exchange and data sharing inherent to fusion centers, the social capital from interpersonal networks, and the trust developed between organizations by working together represent the lateral mechanism domain from the ICC model. The accesses to enhanced analytic capability, exchange of information, and support for many missions across multiple agencies provide incentives, as described in the ICC model. The multiple agencies and disciplines working together in a fusion center help to enable an appreciation for different points of view based on experience and expertise, as well as building trust and a sense of teamwork among colleagues that aligns with the people domain of the ICC model. These last three elements also comport with the ideas associated with the dimensions of mutuality and trust and reciprocity presented by Thompson and Perry.

The collaboration present within state and major urban area fusion centers also includes examples associated with Thompson and Perry's autonomy dimension in collaborative processes. Agencies participating in fusion centers maintain an organizational self-interest identity and a separate identity as part of the collaborative group that is the fusion center. Law enforcement agencies tend to push the fusion center towards a law enforcement centric focus, which aligns with their own interest, while state homeland security agencies may push for a strong commitment to an all-hazards

approach that serves their agency interest. This point of friction between the two points of view is documented in the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (United States. Department of Homeland Security, 2008).

Additionally, the autonomy dimension can be seen between levels of government represented in fusion centers. City and county law enforcement agencies and federal law enforcement agencies participating in a state level fusion center may experience conflict between the interests and priorities of their agencies and those of the fusion center. The challenges inherent to collaboration among different levels of government will be explored in the next section, which explores collaboration and federalism.

C. HOMELAND SECURITY COLLABORATION THROUGH FEDERALISM

The political governance structure of the United States is based on idea of federalism. The concept of federalism is built on the premise that two levels of government exercise sovereignty over the same people in the same territory simultaneously (Clovis, 2006 p. 3). The fundamental basis of this political theory suggests that some level of collaboration exists between the two levels of government in order to exercise power in the same space over the same people. The U.S. model, based on the Constitution, is known as dual-federalism because each level of government exercises the power and provides the services accorded by the Constitution (Clovis, 2006 p. 3).

In a collaborative sense, three domains from the Inter-organizational Collaborative Capacity (ICC) are clearly present within the structure. The ICC domain of purpose and strategy is evident in the evolution from the Articles of Confederation to the establishment of the Constitution. The states abandoned the Articles of Confederation to create a more balanced system, which resulted in the drafting and adoption of the Constitution (Clovis, 2006, p. 3). It provided a better structure for their common purpose and recognized interdependencies such as national defense. The ICC domain of incentives can be seen in the acknowledged benefit of collaboration, which was initially recognized in commerce and national defense. The ICC structure domain is represented by the Constitution, which provides the formalized structure to enable this collaboration.

The Constitution provides for enumerated or specific powers, which are given to the national government, and the Tenth Amendment to the Constitution stipulates that the reserved powers not implicitly granted to the federal government are left to the state governments (Clovis, 2006 p. 4).

The autonomy dimension described by Thompson and Perry also exists within the federalism system of government within the United States. State governments maintain two separate identities, one as a sovereign entity, and another as a member of the United States. Sometimes their self-interests conflict with the interests of the central government. In these cases, the Supreme Court of the United States is identified as the adjudicating body (Clovis, 2006, p. 4).

Since the governmental structure of the United States is rooted in federalism, it provides the framework for the organizational framework for collaboration on homeland security issues between agencies of the federal government and those within state governments and local governments. The premise of this idea rests on the fact that the security and safety of the United States and its citizens is both a mutual goal and responsibility (*National Strategy for Homeland Security: October 2007*). The quality and effectiveness of collaboration within the federalism structure of our government ultimately dictates the degree of success that can be obtained between federal agencies, state, and local governments in achieving homeland security goals and objectives including those related to risk management and intelligence. This idea is supported by the following statement from the National Strategy for Homeland Security:

> Throughout the evolution of our homeland security paradigm, one feature most essential to our success has endured: the notion that homeland security is a shared responsibility built upon a foundation of partnerships. Federal, State, local, and Tribal governments, the private and non-profit sectors, communities, and individual citizens all share common goals and responsibilities – as well as accountability – for protecting and defending the Homeland.
>
> (National Strategy for Homeland Security: October 2007).

National homeland security policy, and by extension its goals and specific programs, do not include state and local governments as full collaborative partners in the homeland security policy model as it exists today. A finding in a Heritage Foundation report states, “Despite being essential and equal partners with the federal government in defending the homeland against terrorism, state and local governments have little say in the development of national policy.” (Mayer, M. A., Carafano, J. J., and Zuckerman, J., 2011). Clovis argues that the attacks of 9/11 resulted in a dramatic power shift in federalism towards a more centralized federal government similar to other times of crisis throughout our history (Clovis, 2006, p. 9). This argument from Clovis fits with the assertion that the federal government’s homeland security policies continue to encroach on the activities that have previously been the purview of state and local governments (Mayer, M. A., Carafano, J. J., and Zuckerman, J., 2011).

This centralization of power in the federal government has left state and local government with a diminished voice on homeland security policy issues (Mayer, M. A., & Baca, L., 2010). This translates directly to the risk analysis and management within the homeland security enterprise. DHS acknowledges the need to include more state and local threat and risk information into its assessments by establishing a goal to do so (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010, p. 59). Additionally, a DHS official is quoted as saying that state and local risk and threat information was not being included in federal assessments in a meaningful approach in a 2007 report from the Congressional Research Service (Masse, T, Rollins, J, and O'Neil, S, 2007).

State and local homeland security activities tend to be more driven by grants than by risk management priorities. A review of documents such as the *National Preparedness Goal*, *Homeland Security Presidential Policy Directive 8*, *Target Capabilities List*, and homeland security grant guidance provided to the states support this observation. Clovis makes an argument and provides evidence to support his claim that grant programs provide the vehicle by which the federal government preempts local and state prerogatives through the dictation of special requirements to achieve specific goals (Clovis, 2006). These arguments and on-going friction within the U.S. system of

federalism emphasizes how inadequate communication and coordination of information, organizational distrust, competition for resources, and arrogance can negatively impact collaboration.

The existing homeland security policy system includes a number of "barrier factors" that impede effective collaboration within the federalism system. Clovis stipulates, "The major tensions in the past, continuing to present times, have been related to the struggle for power between the states and central government." (Clovis, 2006, p. 4). State and local government's limited ability to comment on homeland security policy after it has been discussed, drafted, developed, and circulated coupled with the filtering and editing of input to policy committees from state and local governments is disingenuous to the policy-making process (Mayer, M. A., & Baca, L., 2010). Bellavita postulates the national government has embraced the opportunity to decide what is best for homeland security through default, arrogance, and careerism of federal leadership (Bellavita, 2005, p. 7). Clovis explains that certain aspects of the existing structure represent coercive federalism to include stronger and tighter conditions of grant-in-aid programs and preemption of state choices, federal judiciary interference in the business of state and local government, and greater use of under- or unfunded mandates to coerce action within state and local governments (Clovis, 2006, p. 8). Bellavita describes the existing homeland security organizational paradigm as "a well oiled machine steered by an informed central authority," and he goes on to explain the federal government remains entrenched in their hierarchal system with a fear based on not trying or being able to control everything (Bellavita, 2005, p. 7). These issues undermine collaboration between federal agencies, state, and local governments by fostering many of the "barrier factors" listed in Table 2.

While the existing variation of federalism represents significant challenges to collaboration among the different layers of government within the United States, changes can be made to the system to enable stronger collaboration, and hence, improve the efficiency and effectiveness of homeland security. Clovis points out that a tradition of collaborative federalism exists in long-standing arrangements between the Federal Emergency Management Agency (FEMA) and the Center for Disease Control and

Prevention (CDC) (Clovis, 2006, p. 13). Matt Mayer and Sheriff Baca suggest that a many of the vital tasks within the national homeland security enterprise are decentralized, and that success of the enterprise requires greater information sharing, robust state and local representation as full partners, and a shift away from the rigid federal-centric approaches (Mayer, M. A., & Baca, L., 2010). Clovis proposes that congress through its executive agent DHS should provide leadership through facilitation instead of directing by providing guidelines, milestones and funding in the form of block grants; and that state and local governments are positioned with greater flexibility to implement programs and thus should collaborate vertically, horizontally, and with other jurisdictions to facilitate the flow of information and the most efficient and effective implementation programs (Clovis, 2006, pp. 17–18). The Interagency Threat Assessment and Coordination Group (ITACG) is model that incorporates state and local perspectives in the intelligence process, and indicate this model should be emulated to foster greater involvement of state and local partners in shaping homeland security policy and priorities (Mayer, M. A., Carafano, J. J., and Zuckerman, J., 2011). These ideas represent an opportunity to embrace the "success factors" for collaboration while managing the "barrier factors."

As the foundation for the relationship between state and local government and the federal government of the United States, federalism provides the conceptual framework in which collaboration between these levels of government must occur. The federalism concept as it exists in the American experience includes both enabling and barrier factors. Effective collaboration for homeland security risk management will require strategic planning and thought to exploit the enabling factors and manage the challenges. The next two sections provide a discussion of strategic planning and thought, and offer ideas on how to leverage these concepts and principles to advance collaborative efforts between intelligence and risk management.

D. APPRECIATIVE INQUIRY, THE CYNEFIN FRAMEWORK, AND STRATEGIC PLANNING FOR STRATEGIC COLLABORATION

The homeland security enterprise exists as a complex adaptive system in which risk management plays a central role. This complex environment presents many

competing priorities, demands for resources, and opportunities that must be balanced to consider multiple man-caused and natural threats in a dynamic political and social environment (United States Department of Homeland Security (DHS), 2011). Risk management provides the process to include these factors in the discussion and decision making at the strategic, operational and tactical levels. The discourse afforded by risk management enables the development and joint pursuit of state, regional, and national goals and objectives for homeland security. Effective collaboration for risk management provides the vehicle to achieve equilibrium amid these competing factors. Principles of strategic thought and planning are required to enable the collaborative processes demanded for homeland security risk management.

Collaboration requires elements of structure and strategy to achieve the results desired by the entities invested in the collaborative process. The field of strategic planning offers several ideas and theories that can be leveraged to improve the collaborative effort to strategically manage risk within the homeland security domain. This chapter explores how strategic thought and planning principles, the concept of Appreciative Inquiry, and the Cynefin Framework can work together to improve collaboration and the strategic approach to risk management.

1. Appreciative Inquiry

The concept of appreciative inquiry provides an approach to improve system capability through asking questions to seek information and better a better understanding of the environment. Barrett and Fry define Appreciative Inquiry (AI) as, "a strength-based, capacity building approach to transform human systems toward a shared image of their most positive potential by first discovering the very best in their shared experience" (Barrett and Fry, 2005, p. 25). AI exudes collaboration by fostering a dialog among cooperative members to capture examples of past and present success stories, organizational pinnacles, and epiphanies to replicate and adapt them to improve systems and discover what is possible. This foundation provides an environment that encourages investing social capital and exchanging best practices among organizations.

While actively promoting collaboration, the appreciative inquiry concept also limits "barrier factors." The AI process seeks system improvement by focusing and building on positive attributes instead of defining and fixing deficiencies (Barrett & Fry, 2005, p. 31). This shift in discourse from "fixing problems" to "replicating success" frames collaborative conversations in a positive manner, thus promoting trust and the free exchange of information and ideas. AI also avoids fragmentation by focusing on systemic and organizational improvement instead of the traditional analytic approach of breaking problems down into component parts creating specialization and trend towards myopic focus (Barrett & Fry, 2005, p. 30). Specialization and too much attention to the subcomponents of complex problems can produce divergent goals and blurring of goals, which become barriers to effective collaboration. The manifestation of this problem can be seen in both the risk management an intelligence communities. The specialization of the collection disciplines and analysis disciplines often puts intelligence interests at odds or in competition with one another (Lowenthal, 2009). A similar situation exists among for risk analysts within the homeland security community (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). Appreciative inquiry can also act to reduce over dependence on experts and hierarchy and reduce defensive posturing when problems or deficiencies are identified (Barrett & Fry, 2005 pp. 31–32). This in turn can assist in managing the competition within the intelligence community and the risk assessment community and helps foster trust and open communication thus reducing barriers associated with rigid structure.

2. The Cynefin Framework

The Cynefin framework provides a framework that helps collaborative groups or organizations make sense of dynamic and complex issues through group interaction. Categorization is not the focus for the Cynefin framework; instead the focus is geared towards considering elements of decisions, perspective, conflict, and change. Cynefin comes from a Welch word that loosely translates in English to "habitats," but in this context is better understood as, "the multiple affiliations that profoundly influence what we [*as individuals and organizations*] are but of which we can only be partly aware" (Lazaroff, 2006, p. 66). Kurtz and Snowden specify that the Cynefin framework lends

itself particularly well to collaborative approaches and allowing a sense of shared understanding to emerge through group discourse (Kurtz & Snowden, 2003, p. 468).

The Cynefin approach of social complexity, also known as contingent complexity, includes the concepts of unorder and emergence, while adding other concepts to address the differences between human systems and biological systems. These additional concepts are important for understanding decision making and collaboration and include the following: 1) Humans do not base decisions on rules but rather on pattern association based on their experience or the group narrative; 2) Humans and by extension organizations have multiple personalities that are maintained in parallel and the dominant personality depends on situational context; 3) Humans are self-aware, thus making it difficult to distinguish accidents from planned actions; and 4) Free will allows humans to create order and structure in their interactions (Lazaroff, 2006, p. 70). These factors help define perceptions and shape interactions, bias, filters, and perceptions of individuals and agencies in collaborative environments.

The Cynefin framework, illustrated in Figure 9, includes five separate domains that are divided into ordered, unordered, and disorder. The ordered domains are situated on the right side of the model and include the known causes, effect domain, and the knowable cause and effect domain. The unordered domains are situated along the left side of the model and include the complex relationship domain and the chaos domain. Additionally, the domain of disorder is located in the center of the model. Most people and organizations perceive the top right quadrant “knowable” to be the most desirable, however, there are no values associated with the domains, so no one is actually better than the others. The real value of the model is to facilitate discussion and consensus with uncertain conditions (Kurtz & Snowden, 2003, p. 468).

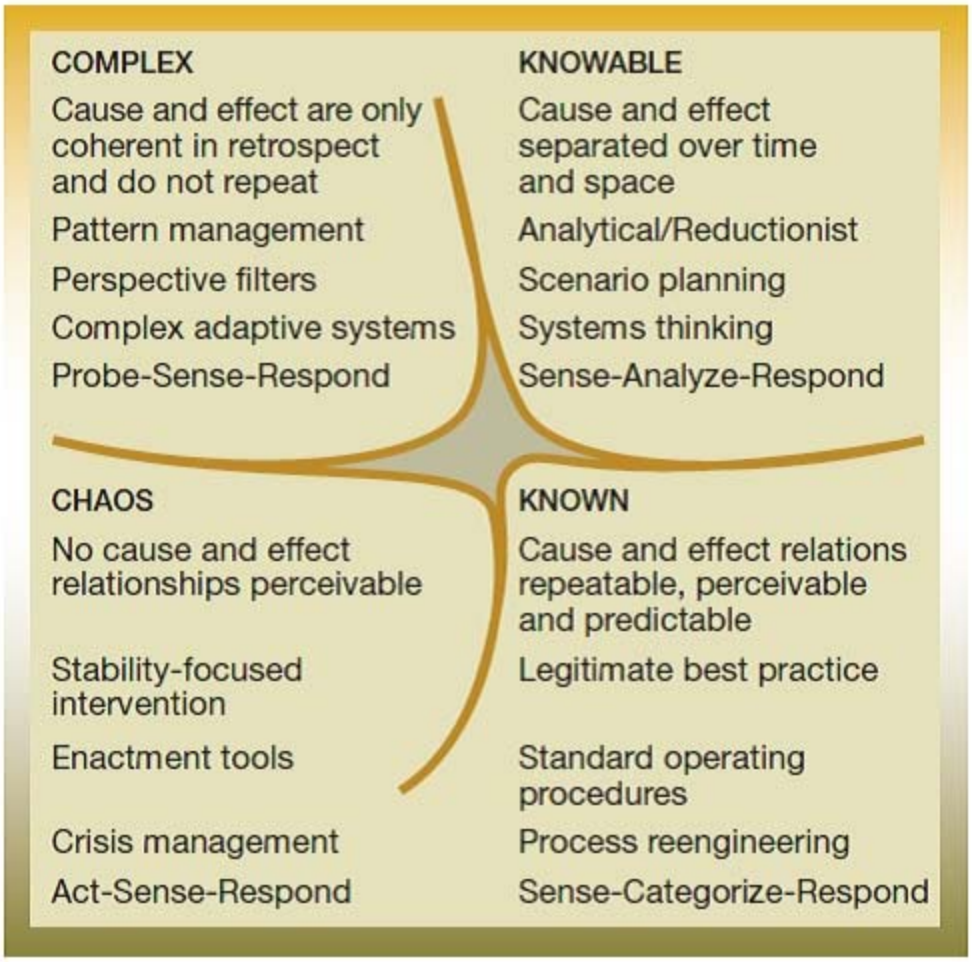

Figure 10. The Cynefin Framework from (Kurtz & Snowden, 2003).

The simplest of the domains is the "known" domain or simple order. The cause and effect relationships associated with issues in this quadrant are linear and empirical, and are not widely open to dispute or varying interpretations. The self-evident nature of the cause and effect relationships lend themselves well to the application of empirically determined best practices and hierarchical management structures (Lazaroff, 2006, p. 66). The focus in this space is on efficiency where incoming data is sensed, categorized, and responded to in accordance with predetermined practices (Kurtz & Snowden, 2003, p. 468). Many tactical risk management issues fit within this domain. Examples include; elevating homes or removing them from floodplains to reduce flood risk or installing security fences to limit access as to improve security at a facility. The simple

relationships and structured decision models indicative of issues in this domain do not lend themselves to collaborative techniques. One could easily see where the structure in this domain could stifle collaboration. The collaborative value of identifying issues that fit within this domain is it allows the group to focus their efforts on issues within the knowable and complex domains.

The domain of "knowable" or complicated order is closely associated with the "known" domain although slightly more complex in nature. The cause and effect relationship associated with issues or decisions within this domain do not present themselves as self-evident like those in the "known," but instead require some level of expert interpretation (Lazaroff, 2006, p. 67). Kurtz and Snowden explain that the issues and decisions within the "knowable" domain can ultimately be moved to the "known" domain with the investment of the appropriate time and resources (Kurtz & Snowden, 2003, p. 468). The decision-making process in this quadrant can be represented by sensing data, apply expertise to analyze the data, and then respond accordingly. Tactical and operational risk management issues often fit within this domain.

Homeland security risk management examples in the "knowable" domain may include a structural and nonstructural seismic analysis of a building to develop a suite of options to improve the seismic performance of a building and options to reduce damage to nonstructural components; or a site security assessment to develop an ensemble of measures that work in concert to improve the security at a facility. Lazaroff indicates that this leads to establishing strong entrained patterns or order that that are subject to validation as good practices, not best practices and once established difficult to disrupt (Lazaroff, 2006, p. 67). Kurtz and Snowden point out the danger with the entrained patterns in which simple errors in assumptions can produce false conclusions that are difficult to isolate and detect (Kurtz & Snowden, 2003, pp. 468–469). Collaboration can be effective in this domain to provide access to the appropriate expertise, evaluate and formulate responses, and track cause and effect relationships.

The “complex” or complex unorder domain represents the quadrant that is home to the issues and decisions where cause and effect relationships exist, but the number of factors and relationship among those factors defy categorization and analytic techniques, thus making patterns difficult to define (Kurtz & Snowden, 2003, p. 469). In this sense, most of the patterns are only discernable in retrospect. This domain includes more strategic homeland security risk management issues, which include examples such as effective strategies for floodplain management within an entire watershed or developing strategies to promote critical infrastructure resilience that accounts for sector and subsector interdependencies. Discovery is the theme of this quadrant as individuals and organizations probe to identify patterns then sense and respond by reinforcing the positive patterns and destroying the negative patterns (Lazaroff, 2006, p. 67). This space demands collaboration in order to gain new and multiple perspectives on issues and decisions with narrative techniques (Kurtz & Snowden, 2003, p. 469). This domain fosters the sharing and appreciation of the different perspectives that collaborating agencies bring to the table and emphasizes qualitative analysis in lieu of quantitative analysis.

The “chaos” or chaotic unorder domain, located in on the lower left portion of the Cynefin model is characterized by turbulence and as the quadrant that is home to the issues and decisions where no perceived cause and effect relationship exists. Lazaroff and Snowden explain that this domain represents both threat and opportunity depending on if the issue is placed within the domain by accident or on purpose. A crisis can bring about a sudden, unanticipated, and confusing decent into this quadrant or conversely, a complex issue can be moved to this domain to disrupt preexisting patterns and elicit original innovative approaches (Lazaroff, 2006, p. 67). The unconventional threat presented by terrorism where an intelligent adversary adapts tactics to counter security measures and responses provides a good example of a homeland security risk that fits within this domain. Another example of a homeland security risk that fits within this domain would be an infrastructure failure that creates impacts across many sectors and subsectors for reasons that are not understood.

The intent of decisions within the "chaos" quadrant is to reduce turbulence through quick and decisive action. The nature of action may differ in that authoritarian approach offers the opportunity to control the decision space in order to transform the issue into the knowable or known domain, while the collaborative approach provides the opportunity to examine multiple interventions to construct new patters moving the issue to the complex domain (Kurtz & Snowden, 2003, p. 469). Ultimately framing issues in this domain can provide a valuable vehicle to break down existing patterns to create novel innovative patterns through collaborative work. When using this quadrant to elicit collaboration, it is important to resist the autocratic tendencies that result from trying to force issues to the knowable or known domains.

The "disorder" domain is the central domain of the Cynefin Framework and lies in the middle between all four other domains. The placement of decisions and issues in this domain indicate confusion or uncertainty over which of the other four domains applies to the situation. Most individuals and organizations can agree on the meaning of the four domains in the context of the issue being considered, however, strong disagreement often occurs on the subtle issues that are found near the center of the Cynefin Framework. Consequently, competition over the interpretation of how these subtle issues fit within the framework is generally driven by the perception and preferences of individuals and organizations based on where they feel most comfortable and empowered within the framework (Kurtz & Snowden, 2003, p. 470). Lazaroff and Snowden point out that the intelligence function largely takes place within this domain, and that natural tendency is towards bias interpretation based on personal or agency penchants. They describe this action in the following terms:

> Highly structured thinkers will tend to interpret the data as supporting their process to manage simple order; experts will require more time and money to analyze the situation; field agents will make multiple small tests by actions or questions to see what is possible; and the charismatic tyrants will interpret any situation as a crisis so they can be given power to act without reference to other authorities.
>
> (Lazaroff, 2006, p. 67).

The conflict and competition inherent to the "disorder" domain provides the opportunity for bias that needs to be accounted for when undertaking collaborative analysis and decision-making activities.

3. Principles for Strategic Collaboration and Planning

The complex risk analysis and management issues coupled with the multiple stakeholders from different tiers of government and the private sector require significant attention to principles of strategic planning and communication for agencies to come together in a collaborative effort. The "success" factors for collaboration and conceptual models like the Cynefin framework cannot create collaboration without strategy, innovation, communication and leadership. These concepts are interrelated, and together provide the essential elements for collaboration to occur.

Strategic collaboration for homeland security includes a number of environmental factors that influence the potential success of collaborative efforts, and the leaders and managers forging collaborative relationships need to focus their efforts on those factors they can control. While managers may not be able to control institutional support for collaboration, they can likely control factors such as planning, conflict management, stakeholder participation and empowerment, and the governance structure for a collaborative organization (Bryson, Crosby, & Stone, 2006, p. 52). These factors within the managerial sphere of influence align with the five dimensions described by Thompson and Perry and within the "success" and "barrier" factors offered by Hocevar, Thomas, and Jansen. Leaders and managers play an important role in facilitating collaboration though these factors, which generally fit within the structure, lateral mechanisms, and people components (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006) and the five dimensions of governance, administration, autonomy, mutuality, and trust and reciprocity (Thomson & Perry, 2006).

Planning plays an important role in developing productive and successful cross-sector collaborative endeavors. Cross-sector collaboration tends to succeed when both deliberate and emergent planning are incorporated into the collaborative planning process. Deliberative planning provides a traditional structured approach to establishing

goals, objectives, milestones and responsibilities, and emergent planning is less structured and occurs over a period of time as a relationship develops through conversation and the inclusion of social networks (Bryson, Crosby, & Stone, 2006 p. 48). Both approaches to planning address a different aspect of collaborative success factors. The deliberate planning approach comports with the success factors the purpose and strategy and structure components while the emergent approach to planning focuses on the success factors associated with lateral mechanisms and incentives. Deliberate planning works best where collaboration is required, such as among departments within an organization, and the lateral relationships inherent to collaborative networks lend themselves to the emergent planning approach (Bryson, Crosby, & Stone, 2006, p. 48). The combination of approaches remains important to collaboration because lateral networks do not replace organizational hierarchy, instead the hierarchical framework should be considered an overlay to the collaborative network. This is an important consideration, since most organizational managers continue to perform the bulk of their work within their organizational hierarchy (Agranoff, 2006, p. 57).

Greater success of collaborative endeavors occurs when the planning includes the perspectives and interests from all stakeholders. The author, Gerald Harris, applies concepts borrowed from quantum physics that support this premise. A key idea he relates applies directly to how organizations can plan for collaboration. Harris describes this idea as “catalytic and kaleidoscopic thinking” in which the concept that two simultaneous observations from different positions can produce two distinctly different observations that are both accurate and true (Harris, 2009, p. 75). In this sense, he promotes the importance of different points of view in the both collaboration and strategic planning. This concept comports with the “success” factors within the incentives and people organizational components described by Hocevar, Thomas, and Jansen. Additionally, this notion is supported by the observation that collaboration is often sought when independent attempts to address an issue or solve a problem have failed or are likely to do so, and these failures cannot be overcome by acting alone (Bryson, Crosby, & Stone, 2006, p. 46).

Large, complex, or "wicked" problems present the greatest challenges to organizations while at the same time provide the greatest opportunity for collaborative solutions. Cross-sector collaborations, meaning partnerships among governmental and private organizations, tend to form during periods of turbulence and uncertainty centered on complex problems (Bryson, Crosby, & Stone, 2006, p. 46). Organizations should embrace the notion that uncertainty cannot be escaped, and that it can provide an opportunity for collaboration. Harris equates the quantum physics concept that it is impossible to know both the position and speed of an electron to uncertainty in the sense of strategic planning (Harris, 2009, p. 43). In this sense, analysis should be viewed as a work in progress because there is always something else to learn and add to the body of knowledge. In the same respect, collaboration within the complex and chaos domains of the Cynefin network should be embraced to further analysis of complex issues and problems.

Collaboration by its nature expands the realm of possibilities, and thus organizations must be willing to explore and accept a broader range of possibilities than they had initially envisioned. This view is supported by association with "success" factors for collaboration to include an appreciation for the perspectives of others and acknowledging the benefits of collaboration (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006, p. 8). From a strategic planning perspective, two concepts highlighted by Harris apply to opening up to a wider range of possibilities. The first encourages organizations to go beyond dualistic thinking, in other words, avoid good/bad or either/or characterizations and encourage learning with more inclusive approaches to thought and examination (Harris, 2009, p. 33). The second is accept that organizations, issues, and problems are interconnected in one space, and so changes to any component within that space create second and third order effects that ripple throughout the whole environment (Harris, 2009, p. 85). The known and knowable domains within the Cynefin Framework provide comfort in the sense that uncertainty is limited. However, too much focus by organizations in these two domains limits collaboration through a failure to explore alternate possibilities, which in turn can lead to arrogance and a false sense of complete understanding.

E. OVERCOMING OBSTACLES AND CHALLENGES TO COLLABORATION

The focus of attention should not be limited to those enabling situations and "success" factors. The understanding and effective management of "barrier" factors must also garner attention, if collaborative action is going to be successful. The act of recognizing these obstacles to collaboration, and then taking the appropriate action to minimize their influence, provides the best avenue to encourage collaboration among agencies with different agendas and priorities.

Establishing mutual trust among organizations in situations where collaboration is desired holds a place of paramount importance and can present a formidable barrier if not managed appropriately. When organizations initiate overtures of collaboration, they should be mindful that reputations and prior relationships play a significant role in establishing trust. Partnering organizations often base their judgments of organizational trustworthiness and legitimacy on prior relationships and networks (Bryson, Crosby, & Stone, 2006, p. 46). Hocevar, Thomas, and Jansen specifically identify organizational-level distrust as a barrier "factor", and several other barrier factors they identify also influence the degree of "trust" or "distrust" such as; competency, arrogance, hostility, animosity, territorial tendencies, inadequate communication and information sharing, and competition for scarce resources (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006, p. 8). Research shows that trust not only plays an important role in facilitating collaboration at the start, but that it plays an important role in holding the collaborative group together, and should be seen as an on-going requirement for maintaining effective partnerships in collaborative efforts (Bryson, Crosby, & Stone, 2006, pp. 47–48).

Conflict between organizational self-interest and collective interest can undermine efforts to build and maintain trust among partners in collaborative organizations if overlooked. Thompson and Perry identify and describe this natural strain that is the result of a dual identity in that organizations involved in collaborative action possess both interests inherent to the specific organization and interests of the collective group, which can be at odds with one another (Thomson & Perry, 2006, p. 26). Effective management of this strife is essential for collaborative success. This can be accomplished through

deliberative and emergent planning processes to equalize power within the group through utilization of stakeholder analyses and responding effectively to the input from primary constituent groups (Bryson, Crosby, & Stone, 2006, p. 48). This builds trust by facilitating communication and valuing the perspectives of other organizations in the group that are identified as "success' factors for collaboration by Hocevar, Thomas, and Jansen.

In his book, *The Speed of Trust,* Stephen Covey identifies three key ideas to improving intent and thereby facilitating stronger communication and hence enabling the building of trust. These three concepts are: examination and refinement of motives, clearly stating intent, and to embrace and choose abundance (Covey, 2006, pp. 85–90). First, organizations should regularly evaluate their mission, goals, objectives, and plans to maintain a firm understanding of their motives so that they can be communicated with transparency. Accomplishing this first step allows organizations to clearly state their intentions to the other organizations involved in the collaborative endeavor. Finally, the organization should make a conscious choice to view the situation with an emphasis toward abundance instead of scarcity. Covey points out, in most every situation, abundance is a reality that can produce even more (Covey, 2006, p. 88). This third idea applied to interagency collaboration suggests that there is an abundance of talent, prestige, recognition, and potentially resources to accomplish the work, if collaborating organizations employ genuine communication to make their intent transparent to build the required trust among partners.

F. DECISION MAKING IN A COLLABORATIVE CONTEXT

Deliberate and emergent planning can help alleviate trouble with decision making in collaborative environments; however, several other factors need to be considered to promote trust among collaborating organizations. The governance and administrative dimensions described by Thompson and Perry emphasize the structure components necessary for decision making in a collaborative environment. The authority of agency representatives to make decisions on behalf of their agencies is an important aspect for success in the structural and administrative aspect of collaboration (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006, p. 8). However, several other factors significantly

influence decision making in collaborative environments, and distinct differences exist between public sector organizations and private sector organizations relative to collaborative decision making.

Networks and interdependent relationships inherent to collaboration contain power bases that provide significant influence over the decision-making process. Collaborative networks do alter the perceived public and private boundaries to a certain degree; however, these networks are incapable of replacing public bureaucracy (Agranoff, 2006, p. 62). While research demonstrates private sector participation in collaboration influences public sector decision making, it is also clear that public sector institutions and administrators make and implement decisions in the public domain. Supplying performance and intelligence data represents one way in which private sector can influence decision making in public-private collaborative efforts. The availability of data and intelligence based on data analysis is not as great in the public sector as in the private sector (Nutt, 2006, p. 292). The competition inherent to private sector organizations relies on analysis of large amounts of data, and thus the private sector has a vested interest in gathering and maintaining large data sets. The manner in which the data and analysis from the private sector is presented can influence how it is interpreted and how a decision is made. This concept is described as "choice architecture" in the book, *Nudge*, in which the authors argue that there is no neutral design (Thaler, R. H. & Sunstein, C. ., 2009, .p 6).

Robert Arangoff describes four types of power that coexist with the legitimate power vested in the governance and structure components; these elements of power include; a champion, political core, technical core, and support staff. The power associated with the role of the "champion" comes from the visibility and prestige this person or organization lends to the group, which encourages partners to stay and find a way to cooperate (Agranoff, 2006, p. 61). This relates to the important use of social capital as a lateral mechanism (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006, p. 17). The "*political core"* includes agency leaders who often serve on governance boards, and their legitimate power, control of resources, and support or lack thereof, conveys the importance or insignificance of the collaborative endeavor (Agranoff, 2006, p. 61). This

type of power and influence relates directly with the structure and purpose and strategy components of collaboration described by Hocevar, Thomas, and Jansen.

Significant differences exist between private and public sector organizations relative to the political influence on decision making. Private sector organizations tend to receive the greatest political influence indirectly from internal sources, where political influence on public sector organizations comes from authority vested in the network and users, which ultimately demands more time to balance the needs presented by oversight bodies (Nutt, 2006). The "technical core" often represents workgroups or specific disciplines and draw upon expert power related to narrowly focus superior knowledge of a particular subject matter (Agranoff, 2006, p. 62). The support staff of collaborative groups exercises power in both a formal and informal manner by taking care of the administrative needs to keep the organization intact and moving towards the identified goals and objectives.

The concept of risk also plays a significant role in decision making for both individuals and collaborative groups. Several factors such as trust, control, choice, familiarity, and categorization of risks influence perception of risk. Individuals and groups are more likely to trust assessments of risk in which either they were directly involved or where they had the opportunity to offer comments (Ropeik, 2010, pp. 70–80). Collaborative groups provide an opportunity to share or distribute risk among partners (Thomson & Perry, 2006).

The influence of risk in decision making differs between public and private sector organizations. The relevance of this fact relates to the perception and treatment of risk in making decisions in collaboration that involves both public and private sector organizations. Private sector organizations tend to make decisions based on internal data analysis and speculation, which they view as less risky, juxtaposed to the public sector that tend to use a consultative and networking approach that they perceived to carry less risk (Nutt, 2006, pp. 298–299). The speculation aspect of decision making in private sector organizations is similar to the concept of "anchoring." Anchoring is a process where there is a known factor and reasonable adjustments are factored in to estimate an unknown factor (Thaler, R. H. & Sunstein, C. R., 2009, p. 22). Private sector

organizations perceive greater risk from collaboration than public sector organizations, and public sector organization perceive greater risk with independent analysis and speculation. The differences in risk perception between the public and private sector can create friction if not accounted for and managed appropriately, and could be seen as a point of strength by creating balance between the two approaches. Additionally, public sector organizations are more adverse to the potential for controversial decisions than private sector organizations, and public sector organization tend to perceive less risk than private sector organizations when facing comparable decisions (Nutt, 2006, p. 299).

The presentation of risk information also influences the perception and ultimately decisions of people and organizations in a collaborative group. How people and organizations view and think about things depends largely on how they are framed by both those presenting the information and those receiving the information (Ropeik, 2010). Thaler and Sunstein describe three heuristics that help people and organizations frame decisions. These include "anchoring," described above, "availability" in which risk is perceived based on how quickly similar examples can be recalled, and "representativeness" in which comparisons like stereotypes are used to estimate likelihood (Thaler, R. H. & Sunstein, C. R., 2009, pp. 24–31). Along with these heuristics, perception of probability, optimism bias, value described as the endowment effect, and that most people find it difficult to work with and understand numbers can skew sensitivity to real or perceived risk (Ropeik, 2010).

G. OBSERVATIONS AND SUMMARY

Many factors influence the success or failure of collaboration. The homeland security enterprise requires agencies from multiple tiers of government and private sector organizations to collaborate. The significant differences between decision making between public sector and private sector organizations, and their perceptions of risk described by Nutt, can provide a source of strength through balance, however, these differences can also create tension among the partner entities. Tension between partners can create or exacerbate conditions that are identified as "barriers" by Hocevar, Thomas, and Jansen.

Although federalism should be viewed as a collaborative effort among the federal government and the state and territorial governments, old tensions between the federal government and state governments persist. The shift of power to the federal government following the terrorist attacks of 9/11 significantly adds to this tension and is fueled by inadequate communication and coordination of information, organizational distrust, competition for resources, and arrogance. These issues directly align with "barrier" factors identified by Hocevar, Thomas, and Jansen. These barrier factors must be addressed, if an effective level of homeland security collaboration between the federal government and state governments is to be achieved.

The Cynefin framework provides a vehicle to enable strategic thought towards collaborative endeavors, and coupled with strategic planning principles, could improve collaborative efforts between public and private sector partners involved in the homeland security enterprise. Significant homeland security issues typically fit within the complex or chaos domain of the Cynefin framework. Additionally, collaboration comports most readily with the complex and chaos domains as well. The framing of homeland security issues, such as risk analysis and management in this manner, can be leveraged to improve collaboration among the multiple partners involved. The goal of moving issues from the chaos and complex domains to the knowable and known domains within the Cynefin framework can help facilitate collaboration by aiding in defining purpose and strategy and creating structure.

V. CONCLUSION AND RECOMMENDATIONS

Risk management within the homeland security enterprise remains too diverse and interdependent to succeed without effective collaboration between disciplines and tiers of government. The risks considered by the homeland security enterprise include catastrophic natural disasters, man-made hazards, and acts of terrorism (*National Strategy for Homeland Security: October 2007 .p 3*). The observations and findings related to intelligence and homeland security risk management discovered in this thesis fit within one of the three domains of the Inter-Organizational Collaborative Capacity (ICC) Model from Hocevar, Thomas and Jansen. These three domains include purpose and strategy, structure, and lateral mechanisms. The domains of incentives and people tend to apply more directly to the individual within organizations and thus fall outside the focus of this thesis.

A. PURPOSE AND STRATEGY

A successful model for collaboration for homeland security risk management must begin with a common purpose and strategy that establishes the foundation to unify effort among a wide dichotomy of interests and stakeholders. Several factors influence the ability to develop a common purpose and strategy, such as recognize interdependencies and common interests among organizations, adaptability to the interests and priorities of other organizations, and the sense of a need to collaborate as the issue at hand is too large and complex to handle alone (Hocevar, S. P., Thomas, G.,F., & Jansen, E., 2006). This step also supports a strategic approach by communicating intentions, planned actions, and perceptions of reality. This communication enables dialog on core beliefs, assumptions, and values to ensure organization priorities, goals, and objectives remain true and grounded (Harris, 2009). The following conclusions fit within the purpose and strategy domain of collaboration.

Homeland security strategy and guidance documents identify risk management as an important concept central to all areas of the homeland security enterprise.

Risk management remains a central theme and point of emphasis for strategy and guidance documents throughout the homeland security enterprise. The National Infrastructure Protection Plan (NIPP) identifies its risk management framework as the cornerstone of the entire infrastructure protection strategy (*National Infrastructure Protection Plan*, 2009, p. 27). The Homeland Security Strategy acknowledges that risk management transcends all aspects of homeland security and factors significantly into resource allocation decisions for the elimination, mitigation, and control of risks (*National Strategy for Homeland Security: October 200,7 .p 41*). Risk management concepts constitute the basis for state and local all-hazard mitigation plans, which includes a strategic planning process, risk identification and assessment, development of mitigation strategies, and a review process to monitor progress towards risk reduction (Federal Emergency Management Agency (FEMA), 2007). The fiscal year 2011 grant guidance from FEMA for the Homeland Security Grant Program (HSGP) includes developing a Threat Hazard Identification and Risk Assessment (THIRA) as the first objective under the first priority to advance the whole of community approach to emergency management and homeland security. The development or improvement of the THIRA will support risk management activities through strategy development, planning activities, investment justifications, and capability gap analysis (U.S. Department of Homeland Security, 2011b). This emphasis also appears in the 2011guidance for the Emergency Management Performance Grant (U.S. Department of Homeland Security, 2011a).

Homeland security strategy documents acknowledge that partnerships and collaboration among public and private stakeholders from all levels of government are required to be effective in managing risks.

Without exception, all homeland security strategy documents reviewed for this thesis recognize that the understanding and management of homeland security risks is far too immense for any one organization or tier of government to accomplish alone. This common theme among the various homeland security strategy and guidance documents is reflected in this statement from the National Strategy for Homeland Security:

> Throughout the evolution of our homeland security paradigm, one feature most essential to our success has endured: the notion that homeland security is a shared responsibility built upon a foundation of partnerships. Federal, State, local, and Tribal governments, the private and non-profit sectors, communities, and individual citizens all share common goals and responsibilities – as well as accountability – for protecting and defending the Homeland
>
> (*National Strategy for Homeland Security: October 2007, p. 4*).

This theme is further echoed by the first strategic theme "Broader Collaborative Partnerships" from the NEMA white paper that outlines recommendations for a national mitigation effort (NEMA, 2009).

The U.S. Department of Homeland Security has made significant progress in their efforts to improve risk management and secure its position as core element of the homeland security culture, however significant work remains.

DHS made significant steps towards improving the risk management culture within the homeland security enterprise with the publication and update to the *DHS Risk Lexicon* and the *Risk Management Fundamentals: Homeland Security risk Management Doctrine 2011*. The importance of the DHS Risk Lexicon in advancing the risk management culture within homeland security is best summarized in a statement from Undersecretary Rand Beers in the preface. Mr. Beers states,

> Clear and unambiguous communication among homeland security risk practitioners, decision makers, and stakeholders is necessary to achieve integrated risk management. The DHS Risk Lexicon supports integrated risk management by defining a single language for risk management and analysis. The DHS Risk Lexicon makes available an official set of harmonized risk-related terms and definitions.
>
> (United States. Department of Homeland Security (DHS), 2010).

The homeland security risk management doctrine provides an authoritative on the principles and processes for homeland security risk management and provides the foundation for risk management partnerships throughout the homeland security enterprise (United States Department of Homeland Security (DHS), 2011).

Even with this, notable progress by DHS additional work remains. These documents are still relatively new and do not have the familiarity or the number of users that other strategic level documents within the homeland security enterprise do. FEMA's guidance for state and local mitigation planning was published the same year as the initial version of the DHS Risk Lexicon; however, it makes no references to the DHS Risk Lexicon (Federal Emergency Management Agency (FEMA), 2007). The absence of references to the DHS Risk Lexicon in guidance and strategy document marginalizes it utility, and consequently is remains largely unknown and lightly employed by state and local governments. Curiously, state and local governments are left out as a primary audience for the DHS Risk Management Doctrine, but the document does include a note indicating that these levels of government may find the information useful (United States Department of Homeland Security (DHS), 2011 pp 6).

B. STRUCTURE

Structure builds on the common purpose and strategy to enable willing organizations to collaborate on issues of shared interest. Organizational design, flexibility, metrics and individual support of collaborative efforts are key aspects of this collaborative domain (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011, p. 3). The influence of this domain significantly influences the degree of success of homeland security risk management collaborative efforts. The following conclusions pertain specifically to the structure domain of collaboration.

The existing centralization of homeland security risk management at the federal level of government limits collaboration and stifles strategic risk management within state and local government.

A strong hierarchical organizational structure with centralized power and decision making presents more barriers to effective collaboration than a decentralized approach, and thus centralization of homeland security risk management within DHS remains less effective than decentralizing risk management to state governments and multi-state regional networks. Collaborative endeavors are more difficult to implement across hierarchical organizations (Thomson & Perry, 2006). The focus of the hierarchical

homeland security structure at the federal level appears to be focused on controlling the homeland security priorities and activities of state and local governments instead of seeking their input for developing strategies to manage homeland security risk. DHS authorities told state and local officials they would be actively consulted, but evidence has proven that top-down direction and large amounts of federal funding are used to steer state and local governments marginalizing any shared decision making and leaving little room for independent action and initiative (Edwards, 2007, p. 33).

The existing hierarchical structure of homeland security is more focused on metrics related to grant spending than metrics associated with risk management. Instead of managing homeland security risk, the existing hierarchical homeland security apparatus is designed to create and follow rules and to spend money through federal grant programs (Bellavita, 2005). DHS employs risk assessment in determining the allocation of homeland security grant funds to state and local governments. The existing risk-based grant methodology ignores vulnerability essentially communicating that all states are equally vulnerable (Government Accountability Office (GAO), 2008, p. 4). This negates the concept of applying risk management practices to inform decisions and apply limited resources to address the most significant risks identified by state and local partners.

The homeland security enterprise includes a series of grant driven metrics that provide the basis for collaboration on homeland security issues between state and local governments and the federal government. Homeland security grant programs to state and local governments provide the basis for collaboration in the homeland security domain, and the compliance requirements for these programs demonstrate a complete lack of awareness and sensitivity to homeland security management priorities and the operational activities of state and local governments (Clovis, 2006). These conditions promote divergent goals between state and local governments, and those of the federal government; show disinterest on behalf of the federal government in adapting to the interests of state and local governments; stimulate competition among states for scarce resources; and impose highly structured rules and policies that impede collaboration. All of these conditions align with those identified as barriers to collaboration (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006).

The fusion of the intelligence cycle and risk management process to enable intelligence-led risk management will benefit both the risk management and intelligence disciplines.

Capitalizing on the similarities between the intelligence cycle and the risk management process by combining these models will enhance collaboration between the intelligence and risk management communities resulting in an intelligence-led approach to risk management. The need to improve cross-discipline familiarity between the intelligence and risk management disciplines has been identified and DHS should take steps to address this need through education, training, exchanges, liaison, and transparency (Baker et al., 2009). The fusing of the intelligence cycle and risk management process will significantly advance efforts to improve familiarity by providing a common frame for training and education, improving existing linkages for liaisons to exploit while increasing transparency between the two disciplines.

The risk analysis and assessment provide some tools and concepts that can assist the intelligence community improve their conclusions, and thus their support of homeland security risk management. Risk analysis plays a central role in identifying scenarios and issues of greatest concern for risk management. This information also aids intelligence analysts to concentrate their efforts on producing assessments for the scenarios of greatest concern and directing future collection efforts to refine and improve these (Willis, 2007, p. 14). This fits with the idea that intelligence collectors need to be acutely aware of the daily needs of their customers and working in the spaces of their customers to develop a better contextual understanding of their intelligence needs (Steele, 2002 pp. 154–155). The intelligence-led mitigation approach supports a shift from a supply and demand relationship towards a mutually beneficial relationship that emphasizes shared learning. This shift promotes collaboration and improves the quality of threat assessments (Baker et al., 2009, p. 9).

State and major urban area fusion centers provide the best vehicle to implement intelligence-led risk management to promote the construction of a realistic national homeland security risk management strategy in which state and local governments are equal partners with the federal government.

State and major urban area fusion centers are designed and structured to meet the intelligence needs of the governments they serve. This reality gives them the unique perspective of being closer and more directly invested with the state and local risk management priorities and connectivity to local information sources to support more accurate threat assessments. DHS offers baseline capabilities intended to support the design and intelligence operations of fusion centers to address common needs of the governments they support. While the baseline capabilities offered by DHS provide for some consistency, the state and local governments who own and operate the fusion centers, structure them and prioritize their tasks to meet their unique needs and challenges (United States. Department of Homeland Security, 2008). Mayors and Governors can leverage these fusion centers to provide the necessary intelligence relevant to supporting their risk management decisions (Chen, 2009).

The U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) demonstrates how effective this decentralized approach can be. The MSRAM process provides continuous collaborative interaction between national intelligence analysts and local stakeholders who provide locally available unclassified information (Baker et al., 2009, p. 66). The direct continuous interaction between the intelligence analysts and those charged with managing risk within state and local government that the MSRAM process provides is similar to the relationship fusion centers share with the governments they support. State and local fusion centers provide the conduit connecting the national intelligence community with the analysts and information available within state and local governments to support the all-hazards all-threats risk management information needs of mayors and governors (Steiner, 2009, p. 2). The MSRAM process puts a premium on the information and interaction with state and local officials and provides a vehicle to support local operational and tactical risk management objectives while rolling the information up to the national level to support strategic risk management decisions (Baker et al., 2009 pp. 66–67).

Decentralization of intelligence support for risk management through the network of state and local fusion centers will improve the quality of both intelligence and risk assessments while fostering greater collaboration between the intelligence community and risk management community. A statement from the author, Robert D. Steele, captures the spirit of this idea. He wrote, "Above all, having the distributed network in place, with trusted relationships and pre-approved access, becomes more important than any sort of *central* intelligence organization.....we still need a *national* intelligence agency, but it should be at the center of a *distributed* network." (Steele, 2002, p. 153)

The Cynefin Framework provides a strategic thinking tool to enable the structural flexibility needed for the dynamic reality of homeland security risk management.

Risk management for the homeland security enterprise is a complex adaptive system comprised of many organizations across multiple tiers of government and the private sector working together to manage a multitude of diverse risks. The U.S. homeland security enterprise is filled with competing requirements, interests, goals, and objectives with threats spanning acts of terrorism, malicious cyber activity, pandemics, transnational crime, and natural disasters (United States Department of Homeland Security (DHS), 2011). This complex environment includes multiple interdependencies that add to the intricacy of managing homeland security risk (*National Infrastructure Protection Plan,* 2009). The concept of homeland security enterprise describes to the collective efforts and shared responsibilities of all tiers of government, nongovernmental and private sector partners to develop and maintain the capabilities necessary to manage these risks (United States. Department of Homeland Security, 2010, p. 12).

The unordered domains of complex relationships and chaos within the Cynefin Framework provide a useful medium to examine the intricate nature of risk management relationships in the homeland security enterprise. The homeland security environment includes many dynamics, which include new and emerging technology in the creation of new relationships and interdependencies and asymmetrical threats from intelligent adversaries. Risk analysis is generally based on expert opinion that is rooted in historically stable patterns, such as statistical analysis for determining flood risk. This

traditional approach does not enable the stakeholders involved with risk management to recognize and adapt to unexpected patterns such as one expects to find associated with the dynamic environment with homeland security risk (Kurtz, C.,F. & Snowden, D.,J., 2003, p. 469). Probabilities and vulnerabilities are closely associated with recognized patterns for the purpose of risk analysis (Committee to Review the Department of Homeland Security's Approach to Risk Analysis, 2010). In contrast, the complex relationship quadrant in the Cynefin Framework creates probes to make alternate patterns and potential patterns more visible to gain multiple perspectives to the issue being examined (Kurtz, C. F. & Snowden, D. J., 2003, p. 469). These multiple perspectives provide a larger spectrum of expert opinion that is critical for understanding complex relationships, such as those found within homeland security risk management. The chaos environment within the Cynefin Framework also provides a workspace that can be utilized to explore new possibilities and create the conditions necessary for innovation (Kurtz, C. F. & Snowden, D. J., 2003, p. 469). Learning to accept and leverage chaos is required where creativity is valuable in solving complex problems like one expects within the domain of homeland security risk management (Brafman, Ori & Beckstrom, Rod, A., 2007, p. 203).

C. LATERAL MECHANISMS

Lateral mechanisms represent and important aspect of collaboration within the homeland security enterprise that must be considered and employed in efforts to advance intelligence and risk management activities. They refer to the social networks that exist between individuals in an organization and those in other organizations thus creating formal and informal links between organizations (Hocevar, S. P., Jansen, E., & Thomas, G. F., 2011, p. 3). The following findings pertain to ways in which lateral mechanisms can be leveraged to improve collaboration in the intelligence and risk management aspects of homeland security.

State and major urban area fusion centers provide an effective mechanism to employ collaborative tools and technologies, promote information sharing, and facilitate collaborative learning to advance intelligence and risk management activities.

State and major urban area fusion centers remain a focal point for developing a "trusted" relationship for exchanging intelligence and risk information between the federal government and state and local governments. The rise of fusion centers after the terrorist attacks of 9/11 indicate a recognition that nontraditional actors, such as state and local law enforcement and public safety organizations have an important role to play in the homeland security mission (Masse, Todd., Rollins, John., 2007). This acknowledgement begins the process to establish trust between the intelligence community and state and local personnel associated with fusion centers. The building of trust through social networking among state and local fusion centers and the intelligence community was further advanced by Presidential order in 2005. The 2005 memorandum from the president specified that state and local governments must be treated as full and trusted partners with the federal government in efforts to combat terrorism (United States Department of Homeland Security, 2008, pp. 2–3). This position is further strengthened by the *National Strategy for Information Sharing* which emphasizes a trusted national information sharing capability through an integrated network of state and major urban area fusion centers (*National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing*, 2007). The evolution of this new dynamic between local and state governments and federal agencies continues to show the growth of trust. The Director of National Intelligence's new strategy, "*Strategic Intent for Information Sharing"* includes language referring to state and local governments as trusted partners with interests and responsibilities for optimizing intelligence and information sharing in a responsible manner (*United States Intelligence Community Strategic Intent for Information Sharing*, 2011).

State and major urban area fusion centers demonstrate the effectiveness of lateral mechanisms to facilitate collaborative intelligence work and risk management efforts. These fusion centers were created with the purpose of facilitating a trusted exchange of information between the intelligence community and state and local government. Fusion

centers provide an environment where local, state, and federal public safety personnel and law enforcement intelligence analysts are collocated together on common issues (United States Department of Homeland Security, 2008). The fusion centers provide a venue for continuous interaction between local, state, and federal partners from both the intelligence and risk analysis communities. The continuous interaction builds social capital and facilitates effective communication and technical interoperability which are enabling factors for successful collaboration (Hocevar, S. P., Thomas, G. F., & Jansen, E., 2006, p. 8). This continuous interaction is shown to provide the best communication and collaboration between intelligence and risk analysts and yields the greatest incentives for marinating trust and an effective working relationship (Baker et al., 2009, pp. 24–26).

A state driven comparative risk ranking model can be the vehicle to employ lateral mechanisms to advance homeland security risk management.

A comparative risk ranking and management model provides a mechanism to employ lateral mechanisms effectively to promote collaboration for homeland security risk management. Given the wide spectrum of risks associated with the homeland security domain, they must first be grouped into categories and common attributes identified. Comparative risk ranking promotes the effective exchange of information and transparency by using select common attributes as a point of comparison among seemingly divergent risks (Morgan et al., 2000, p. 49). A comparative approach to risk management promotes an open dialog among all stakeholders, which is a key element of NEMA's recommendations for a national mitigation strategy (NEMA, 2009, p. 4).

Social capital plays an important role in the comparative risk management process. The comparative dialog in comparative risk ranking emphasizes value judgments from the experts and panelists involved in the process (Morgan et al., 2000, p. 52). The importance of broad collaborative networks and full spectrum community-to-federal emphasis in a national risk management strategy promotes shared learning about risks and results in a stronger risk management strategy (NEMA, 2009). State and local hazard mitigation planning prescribes an inclusive comparative risk ranking approach to establish mitigation priorities (Federal Emergency Management Agency (FEMA), 2007).

The all-hazard mitigation planning efforts undertaken by state and local governments demonstrate how a comparative risk management process can produce effective long-term risk management strategies (Berke, P, Smith, G, and Lyles, W, 2009).

D. RECOMMENDATIONS

1. Decentralize homeland security risk management, and clearly define the roles of the private sector and local, state, and federal government agencies in the homeland security risk management framework.

Decentralization of homeland security risk management will change the risk management paradigm within homeland security. In lieu of a prescriptive top down approach, risk management should be accomplished by building the strategy from the bottom up. The decentralized approach can be seen as a mosaic, which is constructed from multiple pieces from state and local governments and federal agencies. This national mosaic should be constructed from regional pieces, which are made from state and federal agency risk assessments and management strategies.

While DHS and other federal agencies must continue to develop risk management strategies for risks outside our borders and for their statutory responsibilities, DHS must focus its risk management efforts on producing guidance and assessment tools and techniques for state and local government. Additionally, DHS should support state and local efforts by leveraging national laboratories and technical experts for risk assessment activities.

The decentralized approach to risk management needs to provide generalized goals through federal guidance without being prescriptive. This will afford state and local governments to establish their own goals within this frame. Decentralization also enables state and local government to effectively employ lateral mechanisms to facilitate a collaborative effort for risk management.

2. Improve the coordination and collaboration between the intelligence community and risk analysts to advance homeland security risk management efforts.

Intelligence contributions are an important aspect of homeland security risk analysis. Efforts to improve collaboration between intelligence and risk analysis will significantly improve the quality of assessments for homeland security risk management. The U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) provides a good model of collaboration between intelligence and risk analysis to emulate. State and local fusion centers provide a vehicle for state and local governments to leverage in improving collaborative relationships between intelligence and risk analysis in a decentralized homeland security risk management framework.

State and regional fusion centers provide one possible component of a collaborative model for risk management. However, most of the fusion centers are still in their infancy with significant work remaining to mature in all-risk management. While fusion centers may be part of the solution, their ability to advance strategic risk management also depends on a larger collaborative framework to promote information sharing, best practices, and guide homeland security risk management for all risks.

3. Employ a comparative risk ranking and management model to support strategic risk management throughout the homeland enterprise.

A comparative risk ranking and management model similar to the Carnegie Mellon Risk Ranking Model would help state and local governments with comparing a diverse spectrum of risk as part of their risk management process. Comparison of risk attributes allows different risks to be compared in a standard framework. This approach will also help develop innovative approaches to assessing risk and developing risk management strategies through avoiding reliance on the traditional patterns that drive risk analysis models.

E. FUTURE RESEARCH

The field of homeland security continues to evolve, and the research for this thesis is not exhaustive. While this thesis contributes to the conversation on improving risk management, additional research will benefit the homeland security enterprise. Specifically, additional research should examine homeland security risk management practices within state and local government, risk analysis in complex adaptive systems, such as critical infrastructure protection, and risk management decision making within the homeland security enterprise.

LIST OF REFERENCES

2009 National intelligence: A consumer's guide (2009). . Washington D.C.: United States. Office of the Director of National Intelligence.

Agranoff, R. (2006). Inside collaborative networks: Ten lessons for public managers. *Public Administration Review, 66*(, Special Issue: Collaborative Public Management), pp. 56–65.

Ahearne, J. (1993). Integrating risk analysis into public policy. *Environment (Washington DC), 35*(2), 16–20, 37.

Arvai, J. (2003). Using risk communication to disclose the outcome of a participatory decision-making process: Effects on the perceived acceptability of risk-policy decisions. *Risk Analysis, 23*(2), 281-289. doi:10.1111/1539-6924.00308

Baker, J., Wool, M., Smith, A., Kahan, J., Ansel, C., Hammar, P., Phillips, M. (2009). *Risk analysis and intelligence communities collaborative framework final report.* (HSI Publication No. RP08-31-02). Arlington, VA: Homeland Security Institute. Retrieved from www.homelandsecurity.org

Barker, K., & Santos, J. R. (2010). A risk-based approach for identifying key economic and infrastructure systems. *Risk Analysis, 30*(6), 962–974. doi:10.1111/j.1539-6924.2010.01373.x

Barnes, P., Charles, M. B. Branagan, M., & Knight, A. (2007). Intelligence and anticipation: Issues in security, risk, and crisis management. *International Journal of Risk Assessment & Management, 7*(8), 1209.

Barnes, C., Branagan, & Knight. (2007). Intelligence and anticipation: issues in security, risk and crisis management. *International Journal of Risk Assessment & Management, 7*(8), 1209-1223. doi:10.1504/IJRAM.2007.015302

Barrett, Frank J. and Fry, Ronald E. (2005). In Richard Doyle (Ed.), *Appreciative inquiry: A positive approach to building cooperative capacity* (1st ed.). Chagrin Falls, Ohio: Taol Institute Publications.

Bayer, J., & Wahlstroem, B. (1991). Applications of probabilistic risk assessments: The selection of appropriate tools. *Risk Analysis, 11*(2), 239–248.

Bellavita, C. (2005). What is preventing homeland security? *Homeland Security Affairs, I*(1), Article 3. Retrieved from http://www.hsaj.org

Berke, P, Smith, G, and Lyles, W. (2009). *State hazard mitigation plan evaluation and model practices: Analysis of federal mitigation policy in the U.S.: Mitigation plans, expenditures, civic engagement, and local capability.* Chapel Hill, North Carolina: University of North Carolina at Chapel Hill. North Carolina Institute of Disaster Studies.

Brafman, Ori & Beckstrom, Rod, A. (2007). *The starfish and the spider.* Penguin Group (USA).

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2006). The design and implementation of cross-sector collaborations: Propositions from the literature. *Public Administration Review, 66,* 44–55. doi:10.1111/j.1540-6210.2006.00665.x

Buschmann, R. (2002). *Risk assessment in the President's national strategy for homeland security.* (Report for Congress No. RS21348). Washington D.C.: Congressional Research Service.

Caruson, K., MacManus, S. A., Kohen, M., & Watson, T. A. (2005). Homeland security preparedness: The rebirth of regionalism. *Publius, 35*(1, The State of American Federalism, 2004–2005), 143–168.

Casman, E., Morgan, M., & Dowlatabadi, H. (1999). Mixed levels of uncertainty in complex policy models. *Risk Analysis, 19*(1), 33–42.

Caudle, S. (2005). Homeland security: Approaches to results management. *Public Performance & Management Review, 28*(3), 352–375.

Chen, Y. (2009). *Tell me what I need to know: What mayors and governors want from their fusion center.* (Master's Thesis, Naval Postgraduate School (U.S.). Center for Homeland Defense and Security). (public) Retrieved from https://www.hsdl.org/?view&did=33136

Clovis, S. H. (2006). Federalism, homeland security and national preparedness: A case study in the development of public policy. *Homeland Security Affairs, II*(3) Retrieved from http://www.hsaj.org

Comfort, L. K. (2002). Managing intergovernmental responses to terrorism and other extreme events. *Publius, 32*(4, The State of American Federalism, 2001–2002), pp. 29-49.

Committee to Review the Department of Homeland Security's Approach to Risk Analysis. (2010). *Review of the Department of Homeland Security's approach to risk analysis.* No. HSHQDC-08-C-00090). Washington D.C.: National Academies Press (U.S.). Retrieved from http://books.nap.edu/catalog.php?record_id=12972

Covey, S. M. R. (2006). *The speed of trust: The one thing that changes everything*. New York: Free Press.

Cox Jr., L. A. (Tony). (2008). Some limitations of “Risk = threat × vulnerability × consequence” for risk analysis of terrorist attacks. *Risk Analysis: An International Journal, 28*(6), 1749–1761. doi:10.1111/j.1539-6924.2008.01142.x

Cox Jr., L. A. (Tony). (2008). What's wrong with risk matrices? *Risk Analysis: An International Journal, 28*(2), 497–512. doi:10.1111/j.1539-6924.2008.01030.x

Cox, J. L. A. (. (2009). What's wrong with hazard-ranking systems? An Expository Note. *Risk Analysis, 29*(7), 940–948. doi:10.1111/j.1539-6924.2009.01209.x

Critical Infrastructure and Key Resources (CIKR): Protection capabilities for fusion centers [December 2008] [An appendix to the 'Baseline Capabilities for State and Major Urban Area Fusion Centers'] (2008). [An Appendix to the 'Baseline Capabilities for State and Major Urban Area Fusion Centers'] United States. Department of Justice. Global Justice Information Sharing Initiative.

Critical infrastructure protection update to national infrastructure protection plan Includes Increased Emphasis on Risk Management and Resilience. (2010). No. GAO-10-296). Washington D. C.: United States Government Accountability Office.

Cummings, M. C., McGarvey, D. C., & Vinch, P. M. (2006). *Homeland security risk assessment, volume I: Setting*. No. RP05-024-01a). Arlington, VA: Homeland Security Studies and Analysis Institute. Retrieved from https://www.hsdl.org/?view&doc=115582&coll=documents

Cummings, M. C., McGarvey, D. C., & Vinch, P. M. (2006). *Homeland security risk assessment, volume II: Methods, techniques, and tools.* No. RP05-024-01b). Arlington, VA: Homeland Security Studies and Analysis Institute. Retrieved from https://www.hsdl.org/?view&doc=115583&coll=documents

Department of homeland security interaction with state and local fusion centers: Concept of Operations (2008). Washington D.C.: United States Department of Homeland Security. Retrieved from https://www.hsdl.org/?view&did=38781

Deutch, J., & Smith, J. H. (2002). Smarter intelligence. *Foreign Policy*, (128), 64–69.

Dillon, R. L., & Tinsley, C. H. (2008). How near-misses influence decision making under risk: A missed opportunity for learning. *Management Science, 54*(8), 1425–1440.

Earle, T. C. (2010). *Trust in risk management: A model-based review of empirical research.* Blackwell Publishing Inc. doi:- 10.1111/j.1539-6924.2010.01398.x

Edwards, F. L. (2007). Federal intervention in local emergency planning: nightmare on Main Street. *State & Local Government Review, 39*(1, A Symposium: Emergency Preparedness of State and Local Governments), 31–43.

Ezell, B. C., Bennett, S. P., von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic risk analysis and terrorism risk. *Risk Analysis, 30*(4), 575–589. doi:10.1111/j.1539-6924.2010.01401.x

Federal Emergency Management Agency (FEMA). (2003). *Developing the mitigation plan: Identifying mitigation strategies and implementation strategies: State and local mitigation planning how-to guide.* (Government No. FEMA 386-3). Washington D.C.: United States. Federal Emergency Management Agency. Retrieved from http://www.fema.gov/

Federal Emergency Management Agency (FEMA). (2007). *Multi-hazard mitigation planning guidance under the Disaster Mitigation Act of 2000*. Washington, D.C.: United States. Federal Emergency Management Agency. Retrieved from United States Federal Emergency Management Agency: http://www.fema.gov/

Federal Emergency Management Agency (FEMA). (2008). *Using the hazard mitigation plan to prepare successful mitigation projects: State and local mitigation planning how-to guide.* (FEMA No. FEMA 386-9). Washington D.C.: United States. Federal Emergency Management Agency. Retrieved from http://www.fema.gov/

Federal Emergency Management Agency (FEMA). (2009). *Comprehensive preparedness guide (CPG) 101: Developing and maintaining state, territorial, tribal, and local government emergency plans*. Washington D.C.: United States. Federal Emergency Management Agency.

Federal Emergency Management Agency (FEMA). (2010). *Nationwide plan review: fiscal year 2010 report to Congress.* Washington, D.C.: U.S. Department of Homeland Security FEMA.

Florig, K. H., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischoff, B., Fischbeck, P. S. & DeKay, M. L. (2001). A deliberative method for ranking risks (I): Overview and test bed development. *Risk Analysis, 21*(5), 913–921.

Florig, H. K., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischhoff, B., Fischbeck, P. S., & DeKay, M. L. (2001). A deliberative method for ranking risks (I): Overview and test bed development. *Risk Analysis: An International Journal, 21*(5), 913–913.

Gilliard-Matthews, Stacia and Schneider, Anne L. (2010). Politics or risks? An analysis of homeland security grant allocations to the states. *Journal of Homeland Security and Emergency Management, 7*(1, Article 57) Retrieved from http://www.bepress.com/jhsem/vol7/iss1/57

Government Accountability Office. (2008). *DHS risk-based grant methodology is reasonable, but current version's measure of vulnerability is limited.* (Report to Congress No. GAO-08-852). Washington D.C.: United States Government Accountability Office.

Government Accountability Office (GAO). (2008). *Highlights of a forum: Strengthening the use of risk management principles in homeland security.* No. GAO-08-627SP). Washington D.C.: United States. Government Accountability Office.

Government Accountability Office (GAO). (2008). *Homeland security: DHS risk-based grant methodology is reasonable, but current version's measure of vulnerability is limited, report to Congressional Committees.* No. GAO-08-852). Washington D.C.: United States. Government Accountability Office. Retrieved from https://www.hsdl.org/?view&doc=100181&coll=limited

Graham, J. D., & Rhomberg, L. (1996). How risks are identified and assessed. *Annals of the American Academy of Political and Social Science, 545*(, Challenges in Risk Assessment and Risk Management), 15–24.

Hansson, S. O. (2005). Seven myths of risk. *Risk Management, 7*(2), 7–17.

Harris, G. (2009). *The art of quantum planning: Lessons from quantum physics for breakthrough strategy, innovation, and leadership* (1st ed.). San Francisco, CA: Berrett-Koehler Publishers Inc.

Hayes, J. K., & Ebinger, C. K. (2011). The private sector and the role of risk and responsibility in securing the nation's infrastructure. *Journal of Homeland Security and Emergency Management, 8*(1) Retrieved from http://www.bepress.com/jhsem/vol8/iss1/13

Hocevar, S. P., Thomas, G. F., & Jansen, E. (2006). In Beyerlein, M. M., Beyerlein, S. T., & Kennedy, F.A. (Ed.), *Building collaborative capacity: An innovative strategy for homeland security preparedness* (13th ed.) Emerald Group.

Hocevar, S. P., Jansen, E., & Thomas, G. F. (2011). Interorganizational collaboration: Addressing the challenge. *Homeland Security Affairs,* (10 Years After: The 9/11 Essays) Retrieved from www.hsaj.org

Innes, M. (2006). Policing uncertainty: Countering terror through community intelligence and democratic policing. *Annals of the American Academy of Political and Social Science, 605*(, Democracy, Crime, and Justice), 222–241.

Interim national preparedness goal: Homeland security Presidential directive 8: National preparedness (2005). . Washington D.C.: United States Department of Homeland Security. Retrieved from https://www.hsdl.org/?view&did=455391

Jenkins, W. O. (2007). *Homeland security: Applying risk management principles to guide Federal investments: Testimony before the Subcommittee on Homeland Security, House Committee on Appropriations.* (GAO Report No. GAO-07-386T). Washington D.C.: United States. Government Accountability Office.

Johnson, L. K., & Wirtz, J. J. (Eds.). (2008). *Intelligence and national security: The secret world of spies an anthology* (2nd ed.). New York: Oxford University Press.

Jones, R. T. (2011 (May)). Managing disaster risk with ISO 31000. *International Association of Emergency Managers (IAEM) Bulletin, 28*(5), 6.

Jones, T. (2008). Advances in risk assessment for Australian emergency management. *Australian Journal of Emergency Management, 23*(4), 4-8. Retrieved from https://www.hsdl.org/?view&doc=114357&coll=documents

Jordan, A. E. (2010). Collaborative relationships resulting from the urban area security initiative. *Journal of Homeland Security and Emergency Management, 7*(1) Retrieved from http://www.bepress.com/jhsem/vol7/iss1/38

Kamarck, E. C. (2002). *Applying 21st-century government to the challenge of homeland security.* (New Ways to Manage Series Arlington, VA: PricewaterhouseCoopers Endowment for the Business of Government. Retrieved from www.endowment.pwcglobal.com

Kean, T., H., & Hamilton, L. H,. (2004). *9/11 Commission report: final report of the national commission on terrorist attacks upon the United States* (1st ed.). Washington D.C.: United States. Government Printing Office.

Keeney, R. L. (2007). Modeling values for anti-terrorism analysis. *Risk Analysis, 27*(3), 585–596. doi:10.1111/j.1539-6924.2007.00910.x

Keeney, R. (1995). Understanding life-threatening risks. *Risk Analysis, 15*(6), 627–637.

Kettl, D. F. (2006). Managing boundaries in American administration: The collaboration imperative. *Public Administration Review, 66,* 10–19. doi:10.1111/j.1540-6210.2006.00662.x

Kiltgaard, R., & Treverton, G. F. (2003). *Assessing partnerships: New forms of collaboration.* (New Ways to Manage Arlington, VA: IBM Endowment for The Business of Government. Retrieved from www.businessofgovernment.org

Kolasky, B. (2011). *DHS adopting integrated risk management approach*. Fairfax, Virginia: Public Entity Risk Institute. Retrieved from https://www.riskinstitute.org/peri/index2.php?option=com_content&do_pdf=1&id=1083

Kurtz, C. F. & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM Systems Journal, 42*(3), 462–483.

Larsson, A., Ekenberg, L., & and Danielson, M. (2010). Decision evaluation of response strategies in emergency management using imprecise assessments. *Journal of Homeland Security and Emergency Management, 7*(1, Article 53.) Retrieved from http://www.bepress.com/jhsem/vol7/iss1/53

Lazaroff, M., & Snowden, D. (2006; 2005). Anticipatory models for counter-terrorism. e*mergent information technologies and enabling policies for counter-terrorism* (51–73) John Wiley & Sons, Inc. doi:10.1002/047178656X.ch3

Leitch, M. (2010). ISO 31000:2009: The new international standard on risk management. *Risk Analysis, 30*(6), 887-892. doi:10.1111/j.1539-6924.2010.01397.x

Lowenthal, M. M. (2009). *Intelligence from secrets to policy* (4th ed.). Washington, D.C.: CQ press.

Masse, T, Rollins, J, and O'Neil, S. (2007). *The department of homeland security's risk assessment methodology: Evolution, issues, and options for Congress.* (Report for Congress No. CRS Report for Congress, RL33858). Washington, D.C.: Library of Congress. Congressional Research Service.

Masse, T., Rollins, J. (2007). *A summary of fusion centers: Core issues and options for congress.* No. RL34177. Washington D.C.: Congressional Research Service.

Mayer, M. A., & Baca, L. (2010). *Want real homeland security? Give state and local governments a real voice* (Backgrounder No. 2467 ed.). Washington D.C.: The Heritage Foundation. Retrieved from http://report.heritage.org/bg2467

Mayer, M. A., Carafano, J. J., and Zuckerman, J. (2011). *Homeland security 4.0 overcoming centralization, complacency, and politics.* (Heritage Special Report No. SR-97). Washington D.C.: Heritage Foundation. Retrieved from http://report.heritage.org/sr0097

McConnell, M. (2007). Overhauling intelligence. *Foreign Affairs, 86*(4), 49–58.

McGuire, M. (2006). Collaborative public management: Assessing what we know and how we know it. *Public Administration Review, 66*(, Special Issue: Collaborative Public Management), 33–43.

Mcneill, J. B., & Mayer, M. A. (2011). *Two steps backward: Homeland security's Presidential policy directive-8* (Web Memo No. 3225 ed.). Washington D.C.: The Heritage Foundation. Retrieved from http://www.heritage.org/Research/Reports/2011/04/Two-Steps-Backward-Homeland-Securitys-Presidential-Policy-Directive-8

Moore, D., Fuller, B., Hazzan, M., & Jones, J. (2007). Development of a security vulnerability assessment process for the RAMCAP chemical sector. *Journal of Hazardous Materials, 142*(3), 689–694. doi:10.1016/j.jhazmat.2006.06.133

Morgan, M. G., Florig, H. K., deKay, M. L., & Fischbeck, P. (2000). Categorizing risks for risk ranking. *Risk Analysis: An International Journal, 20*(1), 49–58.

Moteff, J. D. (2005). *Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences.* (Report for Congress No. CRS Report for Congress, RL32561). Washington D.C.: Library of Congress. Congressional Research Service.

Mr. Y. (2011). *A national strategic narrative*. Washington D.C.: Woodrow Wilson International Center for Scholars.

Murphy, C., & Gardoni, P. (2006). The role of society in engineering risk analysis: A capabilities-based approach. *Risk Analysis, 26*(4), 1073–1083. doi:10.1111/j.1539-6924.2006.00801.x

National Academies Press (U.S.). (2008). *Department of homeland security bioterrorism risk assessment.* National Academies Press (U.S.). Retrieved from http://books.nap.edu/catalog.php?record_id=12206&utm_medium=etmail&utm_source=National%20Academies%20Press&utm_campaign=New+from+NAP+9.30.08&utm_content=Downloader&utm_term=

National Emergency Management Association. (2009). *Recommendations for an effective national mitigation effort*. Lexington, KY: National Emergency Management Association. Retrieved from http://www.nemaweb.org

National infrastructure protection plan (2009). . Washington D.C.: United State Department of Homeland Security.

National intelligence strategy of the United States of America. (2009). No. 09073540). Washington D.C.: Office of the Director of National Intelligence.

National strategy for homeland security: October 2007 (2007). . Washington D.C.: Homeland Security Council. Retrieved from https://www.hsdl.org/?view&did=479633

National strategy for information sharing: Success and challenges in improving terrorism-related information sharing (2007). Washington D.C.: United States. White House Office. Retrieved from https://www.hsdl.org/?view&did=480495

Nutt, P. C. (2006). Comparing public and private sector decision-making practices. *Journal of Public Administration Research and Theory: J-PART, 16*(2), 289–318.

Pelfrey, W. V. (2005). The cycle of preparedness: Establishing a framework to prepare for terrorist threats. *Journal of Homeland Security and Emergency Management, 2*(1), Article 5. Retrieved from http://www.bepress.com/jhsem/

Police Executive Research Forum. (2005). *Protecting your community from terrorism: Strategies for local law enforcement volume 4: The production and sharing of intelligence*. Washington, D.C.: Police Executive Research Forum, U.S. Department of Justice Office of Community Oriented Policing Services.

Power, M., & McCarty, L. (2006). Environmental risk management decision-making in a societal context. *Human and Ecological Risk Assessment, 12*(1), 18–27. doi:10.1080/10807030500428538

Purdy, G. (2010). ISO 31000:2009: Setting a new standard for risk management. *Risk Analysis, 30*(6), 881–886. doi:10.1111/j.1539-6924.2010.01442.x

The Office of the Director of National Intelligence. (2009). *The national intelligence strategy of the United States of America*. Washington, D.C.: United States Government The Office of the Director of National Intelligence.

Robinson, L. A., Hammitt, J. K., Aldy, J. E., Krupnick, A., & and Baxter, J. (2010). Valuing the risk of death from terrorist attacks. *Journal of Homeland Security and Emergency Management, 7*(1, Article 14)

Ropeik, D. (2010). *How risky is it, really? : Why our fears don't always match the facts*. New York: McGraw-Hill.

Saari, S. C. (2010). *Fusion centers: Securing America's heartland from threats* (Master's Thesis, Naval Postgraduate School). (Approved for public release; distribution is unlimited) Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2010/Dec/10Dec_Saari.pdf

Sagarin, R. (2010). Natural security for a variable and risk-filled world. *Homeland Security Affairs, VI*(3) Retrieved from www.hsaj.org

Sanquist, T. F., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk Analysis, 28*(4), 1125–1133. doi:10.1111/j.1539-6924.2008.01069.x

Sarewitz, D., Pielke, R., & Keykhah, M. (2003). Vulnerability and risk: Some thoughts from a political and policy perspective. *Risk Analysis, 23*(4), 805–810. doi:10.1111/1539-6924.00357

Shanzer, D. H. & Eyerman, J. (2009). *Strategic risk management in government: A look at homeland security.* (Managing for Performance and Results Series Arlington, VA: IBM Center for the Business of Government. Retrieved from www.businessofgovernment.org

Sims, J. E. & Gerber, B. (Ed.). (2005). *Transforming U.S. intelligence*. Washington, D.C.: Georgetown University Press.

Steele, R., D. (2002). Chapter 15: New Rules for the New Craft of Intelligence. *The New Craft of Intelligence: Personal, Public, and Political Citizen's Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, and Corruption* (147). Oakton, Virginia: OSS International Press. Retrieved from https://www.hsdl.org/?view&did=235369

Steiner, J. E. (2009). Needed: State-level, integrated intelligence enterprises. *Studies in Intelligence, 53*(3), 1.

Sutcliffe, K. M., & McNamara, G. (2001). Controlling decision-making practice in organizations. *Organization Science, 12*(4), 484–501.

Swaney, J. A. (1996). Comparative risk analysis: Limitations and opportunities. *Journal of Economic Issues (Association for Evolutionary Economics), 30*(2), 463.

Tarrant, M. (2006). Risk and emergency management. *Australian Journal of Emergency Management, 21*(1), 9–14.

Thaler, R. H. & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness* (Revised & Expanded ed.). New York, New York: Penguin Books.

Thomson, A. M., & Perry, J. L. (2006). Collaboration processes: Inside the black box. *Public Administration Review, 66*(, Special Issue: Collaborative Public Management), 20–32.

Tierney, K. J. (1999). Toward a critical sociology of risk. *Sociological Forum, 14*(2), 215–242.

Townsend, K., Sullivan, J. P., Monahan, T., & and Donnelly, J. (2010). Intelligence-led mitigation. *Journal of Homeland Security and Emergency Management, 7* (1, Article 63)

U.S Department of Homeland Security. (February 2011). *About the homeland infrastructure threat and risk analysis center (HITRAC).* Retrieved from http://www.dhs.gov/xabout/structure/gc_1257526699957.shtm

U.S. Department of Homeland Security. (2011). In FEMA (Ed.), *Fiscal year (FY) 2011 emergency management performance grants (EMPG) program*. Washington D.C.: U.S. Department of Homeland Security. Retrieved from http://www.fema.gov/government/grant/nondisaster.shtm

U.S. Department of Homeland Security. (2011). In FEMA (Ed.), *Fiscal year (FY) 2011 homeland security grant program (HSGP)*. Washington D.C.: U.S. Department of Homeland Security. Retrieved from http://www.fema.gov/government/grant/nondisaster.shtm

U.S. Environmental Protection Agency (USEPA). (1987). *Unfinished business: A comparative assessment of environmental problems.* No. 000R87901). Washington D.C.: US EPA Office of Policy Analysis.

United States Department of Homeland Security (DHS). (2011). *Risk management fundamentals: Homeland security risk management doctrine*. Washington D.C.: U.S. Government Department of Homeland Security.

United States intelligence community strategic intent for information sharing. (2011). No. 11152526 | ID 07-11). Washington D.C.: Office of the Director of National Intelligence.

United States. Department of Homeland Security. (2006). *DHS intelligence enterprise strategic plan*. Washington D.C.: United States. Department of Homeland Security.

United States. Department of Homeland Security. (2007). *Target capabilities list: A companion to the national preparedness guidelines*. Washington D.C.: United States. Department of Homeland Security.

United States. Department of Homeland Security. (2008). *Baseline capabilities for state and major urban area fusion centers: A supplement to the fusion center guidelines*. Washington D.C.: United States. Department of Homeland Security.

United States. Department of Homeland Security. (2010). *Bottom-up review report.* United States. Department of Homeland Security.

United States. Department of Homeland Security. (2010). *Quadrennial homeland security review (QHSR).* Washington, D.C.: United States. Department of Homeland Security.

United States. Department of Homeland Security (DHS). (2010). *DHS risk lexicon.* (DHS Publication Washington D.C.: United States. Department of Homeland Security (DHS).

United States. Office of the Director of National Intelligence. (2008). *United States intelligence community information sharing strategy*. Washington D.C.: United States. Office of the Director of National Intelligence. Retrieved from https://www.hsdl.org/?view&doc=90340&coll=limited

Van der Heijden, K. (2005). *Scenarios: The art of strategic conversation* (2nd ed.). West Sussex, England: John Wiley & Sons, Ltd.

Waugh, W. L., & Streib, G. (2006). Collaboration and leadership for effective emergency management. *Public Administration Review, 66*(, Special Issue: Collaborative Public Management), 131–140.

Weiss, J., & Hughes, J. (2005). Want Collaboration? Accept-and actively manage-conflict. *Harvard Business Review*, , 1–9. Retrieved from http://harvardbusinessonline.hbsp.harvard.edu

Willis, H. H. (2007). *Using risk analysis to inform intelligence analysis*. Santa Monica, CA: Rand Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/working_papers/2007/RAND_WR464.pdf

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis: An International Journal*, *27*(3), 597–606. doi:10.1111/j.1539-6924.2007.00909.x

Wilson, K., Leonard, B., Wright, R., Graham, I., Moffet, J., Pluscauskas, M., & Wilson, M. (2006). Application of the precautionary principle by senior policy officials: Results of a Canadian survey. *Risk Analysis*, *26*(4), 981-988. doi:10.1111/j.1539-6924.2006.00793.x

Zegart, A. B. (2005). September 11 and the adaptation failure of U.S. intelligence agencies. *International Security, 29*(4), 78–111.

Zhang, G., Ma, J., & Lu, J. (2009). Emergency management evaluation by a fuzzy multi-criteria group decision support system. *Stochastic Environmental Research and Risk Assessment, 23*(4), 517-527. doi:10.1007/s00477-008-0237-3

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Erik Dahl
   Naval Postgraduate School
   Department of National Security Affairs
   Monterey, California

4. Glen Woodbury
   Naval Postgraduate School
   Department of National Security Affairs
   Monterey, California